Financial Services Authority

FINAL NOTICE

To: **Nationwide Building Society**

Of: Nationwide House
Pipers Way
Swindon
SN38 1NW

Date: 14 February 2007

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 Nationwide Building Society (Nationwide) a Decision Notice on 9 February 2007 which notified Nationwide that pursuant to section 206 of the Financial Services and Markets Act 2000 (FSMA), the FSA had decided to impose a financial penalty on Nationwide in respect of a breach of Principle 3 of the FSA's Principles for Business which occurred between 1 December 2004 and 1 December 2006.

1.2. Nationwide has confirmed that it will not be referring the matter to the Financial Services and Markets Tribunal.

1.3. Accordingly, for the reasons set out below and having agreed with Nationwide the facts and matters relied on, the FSA imposes a financial penalty on Nationwide in the amount of £980,000.

1.4. Nationwide agreed to settle at an early stage of the FSA's investigation and qualified for a 30% (stage 1) discount under the FSA's executive settlement procedures. Were it not for this discount FSA would have imposed a financial penalty of £1.4 million on Nationwide

2. REASONS FOR THE ACTION

2.1. In the relevant period, Nationwide breached Principle 3 by failing to take reasonable care to organise and control its affairs responsibly and effectively, with adequate risk management systems. Nationwide did not take reasonable care to ensure that it had effective systems and controls to manage the risks relating to information security, specifically the risk that customer information might be lost or stolen. In particular:

a) Nationwide failed adequately to assess the risks in relation to the security of its customer information.

b) Nationwide had procedures in relation to information security which failed adequately and effectively to manage the risks it faced.

c) Nationwide failed to implement adequate training and monitoring to ensure that its information security procedures were disseminated and understood by staff.

d) Nationwide failed to implement adequate controls to mitigate information security risks, to ensure that employees adhered to its procedures and to ensure that it provided an appropriate level of information security.

e) Nationwide failed to have appropriate procedures in place to deal with an incident involving the loss of customer information and, as a result, Nationwide did not respond appropriately and in a timely manner to establish the risks to Nationwide customers of financial crime arising from the theft of a Nationwide laptop computer.

2.2. No amount of security can eradicate the risk that electronic storage devices will be lost or stolen. However, steps can and should be taken to ensure that loss of physical equipment does not compromise customer information. Nationwide's failure to implement robust systems and controls regarding the use and storage of customer information on portable storage devices potentially put customers at an increased risk of being victims of financial crime in the event of loss or misuse of the data. Nationwide's additional failure to respond quickly and appropriately in the first three weeks following the theft of a Nationwide laptop increased the opportunity for the information to be used in a way which might result in financial crime.

2.3. The FSA considers these failings to be particularly serious because:

a) Nationwide is the UK's largest building society and holds confidential financial information for over 11 million customers. Nationwide's customers were entitled to rely upon Nationwide to take reasonable steps to ensure the security of information entrusted to it. Nationwide's failure to have comprehensive information security procedures and controls exposed its customers to the risk of financial crime.

b) The failures occurred following a period of heightened awareness of information security issues as a result of government initiatives, increasing media coverage and an FSA information campaign about the importance of information security within the financial services sector.

c) The systems and controls were such that, when the laptop was stolen, Nationwide was not aware that it contained confidential customer information. For a period of three weeks after the theft of the laptop Nationwide failed to take any steps to investigate whether it contained such information.

d) The cumulative impact of the failings represented a significant risk to the FSA objective of reducing the extent to which it is possible for regulated firms to be used for a purpose connected with financial crime

2.4. Nationwide's failures therefore merit the imposition of a financial penalty. In deciding upon the level of disciplinary sanction, the FSA recognises the following measures taken by Nationwide which have served to mitigate the seriousness of its failings:

a) Nationwide has implemented a range of additional measures to increase security around Nationwide accounts including increased anti-fraud measures and monitoring of suspected fraudulent activity.

b) On notification of the theft of the laptop Nationwide disabled the remote access facility, preventing access from the stolen laptop to live Nationwide systems.

c) Nationwide has written to all of its customers explaining the loss of the information and measures customers can take to minimise the risk of identity theft.

d) Nationwide has confirmed, in accordance with its existing policy, that it will reimburse any customer who can establish that they have suffered financial loss as a result of the theft of the information on the laptop.

e) Nationwide has commissioned a comprehensive review of its information security procedures and controls overseen by an independent third party

2.5. Nationwide has received full credit for settlement of the disciplinary case at any early stage; it has received a 30% discount for settling the case at stage one. Were it not for this discount the penalty would have been £1.4 million.

3. RELEVANT STATUTORY PROVISIONS

3.1. Under section 206(1) FSMA, if the FSA considers that an authorised person has contravened a requirement imposed by or under FSMA, it may impose on him a penalty, in respect of the contravention, of such amount as it considers appropriate.

3.2. Section 2(2) of FSMA includes the FSA objective:

"Reducing the extent to which it is possible for a business carried on by a regulated person … to be used for a purpose connected with financial crime".

3.3. 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".

3.4. The FSA's Principles for Businesses constitute requirements imposed on authorised persons under the Act.

4. FACTS AND MATTERS RELIED ON

Background

4.1. Nationwide is the UK's largest building society with in excess of 11 million customers. As with any retail financial institution, the volume and nature of the information held by Nationwide means that the potential impact on consumers from a failure in its systems and controls is very high.

4.2. In November 2004 the FSA published a report entitled "Countering Financial Crime Risks in Information Security" (the FSA Information Security Report). Since then the FSA has issued a number of speeches and publications to raise awareness within the financial services sector of the need for firms to take action to combat the risks of financial crime. In the period since then, government initiatives have sought to increase awareness of the risks of identity theft, and media coverage of identity theft risks has been widespread. The conduct of Nationwide must be seen in the context of this heightened awareness of the risks surrounding information security.

4.3. In August 2006 a Nationwide laptop was stolen from the home of a Nationwide employee. The laptop contained confidential customer information which could have been used to further financial crime. Nationwide reported the loss of the laptop to the police, the Information Commissioner, and to the FSA.

4.4. Nationwide's general practice is to separate customer information across systems so that account information such as the account balance, PIN number and password are not stored alongside data such as the customer's name, address and account numbers. This control reduces the risk of fraud against Nationwide accounts in the event of data compromise.

4.5. Nationwide failed adequately to consider the wider risks to customer information from Nationwide systems being compromised and, as a result, it failed to put in place appropriate controls and monitoring mechanisms to mitigate these risks. The failure to manage or monitor downloads of very large amounts of data onto portable storage devices meant that Nationwide had limited control over information held in this way or how it was used, increasing the risk that it could be used to further financial crime.

4.6. By reason of the facts and matters set out herein, the FSA considers that Nationwide has contravened Principle 3 of the FSA's Principles. In particular Nationwide:

a) failed adequately to assess the risks in relation to the security of customer information;

b) had procedures in relation to information security which failed adequately and effectively to manage the risks it faced;

c) failed to implement adequate training and monitoring to ensure that its information security procedures were disseminated and understood by staff; and,

d) failed to implement adequate controls to mitigate information security risks, to ensure that employees followed its procedures, and to ensure that it provided an appropriate level of information security.

Principle 3 Breach – Systems and Controls

4.7. Nationwide holds large quantities of sensitive financial and personal information about its customers. It is key to the interests of Nationwide's customers that Nationwide has effective systems to keep the information secure. Nationwide's systems and controls should have been robust enough to anticipate equipment theft or loss and to reduce the risk of sensitive data being compromised as a result of such a loss. Firms should consider where their information risks are, whether from external or internal sources, computer systems, human error, accidental loss or deliberate theft of information. Such risks, particularly human error, cannot be eradicated, but can be managed. Having identified where the risks are, firms should establish and maintain controls to mitigate the risk of such incidents occurring.

4.8. Nationwide breached Principle 3 by failing adequately to assess the risks relating to information security and take reasonable care to ensure that it had adequate procedures to manage those risks, including the risks that electronic equipment containing customer information might be lost or stolen. Further, it had inadequate controls in place to ensure that its procedures would be followed.

4.9. The FSA Information Security Report issued in November 2004 specifically highlighted the danger of reliance on an annual requirement on staff to sign acceptance of corporate policies whose size made their effectiveness questionable. The FSA Information Security Report recommended a range of measures to embed procedures such as training, updates, and testing similar to that used for money laundering training. The FSA Information Security Report also highlighted the risks of staff deviating from procedures. To address this risk, firms must have in place appropriate monitoring and controls to ensure that procedures are followed.

4.10. Nationwide's information security procedures were contained in an unwieldy electronic format. The procedures were held on Nationwide's internal website; they were not housed in a single document. The procedures covered a very broad range of information handling issues. The policy document was not structured in a way which would have enabled staff to identify easily which part or parts of the procedure might be applicable to their particular role. In addition, there was no search facility within the procedures to assist with this.

4.11. The policies contained inconsistencies and lacked any prioritisation; critical steps were given the same prominence as lesser issues. Within Nationwide's procedures, no clear distinction was made between mandatory requirements and guidance on best practice.

4.12. Staff were required to self-certify that they had read and understood Nationwide's procedures for information security. Staff received generic training on the

application of the information security procedures; but no job specific training was provided.

4.13. Having designed and implemented its procedures for information security, Nationwide failed to establish controls adequate to ensure that its procedures were understood, and that staff adhered to these procedures. Controls in this context can include a combination of measures such as: physical and electronic barriers to copying and transmitting information to portable storage devices, monitoring of compliance with procedures (including through management and supervision of staff), conducting random and targeted monitoring to ensure that only necessary data is stored on removable storage devices and that appropriate information security measures are in place and being used.

4.14. In 2004, Nationwide conducted an analysis of the FSA Information Security Report making a number of recommendations. During the relevant period Nationwide took a number of steps to enhance information security including enhancements to patch management, configuration and access management systems. However, it failed to give sufficient consideration to customer information security risks that could arise as a result of its own systems and controls.

Response to the discovery of the theft of the laptop

4.15. The laptop was stolen from the home of a long-standing Nationwide employee who needed to have extensive access to customer data. The fact that the laptop had been stolen was reported promptly. The employee did not, however, inform Nationwide of what was on the laptop. In the three weeks following the theft of the laptop, during which time the employee was abroad on holiday, Nationwide took no steps to investigate what information it contained.

4.16. The FSA Information Security Report specifically highlighted the need for firms to have incident management procedures commensurate with the size of their operations. It also highlighted the need for firms to update their procedures in line with developments in technology and the increasing use of portable storage devices with the capacity to hold large amounts of data. Nationwide had inadequate incident management procedures to deal with the loss of IT equipment.

4.17. This failure to have in place a procedure to investigate the extent of the information contained on the laptop inhibited Nationwide's ability to respond promptly and increased the opportunity for the information to be used to further financial crime.

5. FACTORS RELEVANT TO DETERMINING THE ACTION

Relevant Guidance on Sanction

5.1. 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 by deterring firms who have breached requirements from committing further contraventions, helping to deter other firms from committing contraventions and demonstrating generally to firms the benefit of compliant behaviour.

5.2. The FSA's policy on the imposition of financial penalties is set out in Chapter 13 of the Enforcement Manual (ENF 13) which forms part of the FSA Handbook. Section 13.3 of the Enforcement Manual sets out some of the factors that may be of particular relevance in determining the appropriate level of financial penalty. These have been taken into account by the FSA in determining the appropriate level of penalty in this case. Chapter 13 of the Enforcement Manual at paragraph 13.3.4 states that the criteria listed in the Manual are not exhaustive and all relevant circumstances of the case will be taken into consideration. In determining whether a financial penalty is appropriate and its level, the FSA is required therefore to consider all the relevant circumstances of the case.

5.3. The FSA has had regard to the seriousness of Nationwide's contraventions, including the nature of the requirements breached, the number and duration of the breaches and the number of consumers who may have been impacted. The level of financial penalty must be proportionate to the nature and seriousness of the contravention. Details of the breaches identified in this case are set out above. It is the responsibility of regulated firms to ensure that appropriate systems and controls are in place to control their business and ensure compliance with regulatory requirements.

5.4. Despite Nationwide taking steps to increase security, focusing primarily on anti-fraud and anti-money laundering initiatives around Nationwide customer accounts, the potential impact of the information being used for purposes connected with financial crime in the wider context was high given the number of customers, the type of information which was stolen and Nationwide's initial response to the theft. Throughout the relevant period Nationwide did not take adequate care to consider the risk of loss of customer information. The FSA's risk based approach requires firms to undertake an assessment of financial crime risk and where necessary to implement controls to mitigate the risk.

5.5. Reducing the extent to which it is possible for a firm to be used for a purpose connected with financial crime is one of the FSA's four statutory objectives. The profile of information security and identity theft has increased significantly in recent years. FSA has issued several publications drawing public attention to these risks since November 2004. There have also been numerous high profile articles in the national and trade press, FSA speeches and papers as well as guidance from government and industry organisations. The FSA considers it particularly serious that the firm failed to enhance its procedures to an adequate standard during this period of heightened awareness of information security issues and despite various recommendations by its own staff that the systems and controls around information security could be improved.

5.6. The FSA has had regard to the size, financial resources and other circumstances of Nationwide. Nationwide is the largest building society in the UK. It made profits of approximately £540 million in 2005/2006.

5.7. Since September 2006, Nationwide has taken steps to address the risks to customers by:

a) taking a range of additional measures to increase security around Nationwide accounts including increased anti-fraud measures and monitoring of suspected fraudulent activity.

b) Writing to all of its customers explaining the loss of information and measures customers can take to minimise the risk of identity theft.

c) Affirming its existing policy to reimburse any customer who can establish that they have suffered financial loss as a result of the theft of the information on the laptop.

d) Commissioning a comprehensive review of its information security procedures and controls overseen by an independent third party.

5.8. Throughout the FSA's investigation Nationwide has co-operated fully and worked with the FSA to facilitate an early settlement of this matter.

5.9. The FSA has had regard to previous cases involving breaches of system and control requirements that threaten the FSA's financial crime objective. Nationwide has not been the subject of Enforcement action previously.

6. DECISION MAKERS

6.1. The decision which gave rise to the obligation to give this Final Notice was made by the Executive Settlement Decision Makers on behalf of the FSA.

7. IMPORTANT

7.1. This Final Notice is given to Nationwide in accordance with section 390 of the Act.

Manner of and time for Payment

7.2. The financial penalty must be paid in full by Nationwide to the FSA by no later than 28 February 2007, 14 days from the date of this Final Notice.

If the financial penalty is not paid

7.3. If all or any of the financial penalty is outstanding on 1 March 2007, the FSA may recover the outstanding amount as a debt owed by Nationwide and due to the FSA.

Publicity

7.4. 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 you or prejudicial to the interests of consumers.

7.5. The FSA intends to publish such information about the matter to which this Final Notice relates as it considers appropriate.

8. FSA contacts

8.1. For more information concerning this matter generally, you should contact Catherine Harris (direct line: 020 7066 4872 /fax: 020 7066 4873) of the Enforcement Division of the FSA.

…….

William Amos
FSA Enforcement Division