Financial Services Authority

FSA

FINAL NOTICE

To: CGNU Life Assurance Limited,
Commercial Union Life Assurance Company Limited,
Norwich Union Annuity Limited,
Norwich Union Life and Pensions Limited and
Norwich Union Life Services Limited

(together referred to in this Notice as **Norwich Union Life**)

Of: 2 Rougier Street
York
North Yorkshire
YO90 1UU

Date: 17 December 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 financial penalty on Norwich Union Life.

1. THE ACTION

1.1. The FSA gave Norwich Union Life a Decision Notice on 10 December 2007 which notified Norwich Union Life that pursuant to section 206 of the Financial Services and Markets Act 2000 (the Act), the FSA had decided to impose a financial penalty on Norwich Union Life in respect of breaches of Principle 3 of the FSA's Principles for Businesses which occurred between 1 March 2005 and 30 November 2006 (the Relevant Period).

1.2. Norwich Union Life confirmed on 5 December 2007 that it would 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 Norwich Union Life the facts and matters relied on, the FSA imposes a financial penalty on Norwich Union Life in the amount of £1.26 million.

1.4. Norwich Union Life agreed to settle at an early stage of the FSA's investigation. It therefore 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 £1.8 million on Norwich Union Life.

2. REASONS FOR THE PROPOSED ACTION

2.1. In the Relevant Period, Norwich Union Life breached Principle 3 by failing to take reasonable care to organise and control its affairs responsibly and effectively, with adequate risk management systems. Norwich Union Life did not take reasonable care to establish and maintain effective systems and controls for countering the risks that the firm might be used to further financial crime, specifically the risks relating to the security of confidential customer information and the consequential risk of the surrender of customer policies to third parties impersonating its customers.

2.2. In particular, Norwich Union Life failed to undertake an adequate assessment of the financial crime risks which it faced (in particular the risk to information security), failed to assess whether its existing controls were adequate to manage these risks, and failed to implement adequate and effective procedures to address these risks.

2.3. Norwich Union Life's failures to assess these risks and to implement robust systems and controls to deal with them increased the risk that its business could be used for a purpose connected with financial crime and exposed its customers to the risk of being victims of financial crime.

2.4. These failures were highlighted by a number of actual and attempted frauds committed against Norwich Union Life and its customers in mid 2006. The fraudsters used publicly available information (such as names, addresses and dates of birth) to impersonate Norwich Union Life customers and, in a series of telephone calls to Norwich Union Life's call centres, sought confidential customer information and in some cases succeeded in amending customer records such as address and bank account details. The fraudsters subsequently instructed Norwich Union Life to surrender the proceeds of customers' policies to bank accounts controlled by the fraudsters. Over 632 policies were targeted by the fraudsters and there were 74 fraudulent surrenders amounting to approximately £3.3 million in total. This loss was borne by Norwich Union Life which reinstated its customers' policies in full.

2.5. In addition to its customers' funds, Norwich Union Life holds sensitive financial and personal information about its customers. Regardless of whether a policy was surrendered or not, confidential customer information regarding the policy was disclosed to the fraudsters in almost all of those 632 cases. In some cases, this included the customer's full bank account details. Where such information was disclosed, customers were exposed to an additional, ongoing and unquantifiable risk of identity theft. Norwich Union Life did not consider or assess this additional risk.

2.6. Norwich Union Life also breached Principle 3 by failing to take reasonable care to ensure that it had effective systems and controls in place to enable it to respond in an appropriate and timely manner to the potential and actual risks arising from the series of actual and attempted frauds which occurred in mid 2006. As a result, the weaknesses in the caller identification procedures were allowed to remain in place for a significant period of time. Steps to prevent further release of customer information and/or funds were identified by Norwich Union Life's compliance function (Compliance) shortly after discovery of the first successful frauds, but those key steps were not implemented in a timely manner. Norwich Union Life did not give appropriate priority to the financial crime risks when considering those risks against competing priorities such as customer service. Had these steps been implemented immediately, it is likely that the majority of the breaches of customer confidentiality and the majority of the financial losses would have been prevented.

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

(1) Norwich Union Life is one of the UK's largest life insurance businesses with 6.8 million customers in the UK. These customers are entitled to rely on Norwich Union Life to take reasonable care to ensure the security of customer information and funds entrusted to it. The failure to have appropriate financial crime procedures and controls had the potential to expose its customers to the risk of identity theft and financial loss.

(2) Norwich Union Life was aware that fraud and identity theft were increasing problems for the financial services industry:

(a) both fraud and identity theft had been identified as increasingly important by Norwich Union Life's parent organisation Aviva in 2005;

(b) Norwich Union Life also received warnings from Compliance that its systems and controls surrounding financial crime were not wholly adequate; and

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

(3) On discovering the frauds in July 2006, Norwich Union Life took specific action to identify, inform and protect all current and former directors of Norwich Union Life and the wider Aviva Group (Aviva Directors) who were policyholders. It did not take equivalent action at that time to inform and protect the policyholders who were not connected with the business. Of the 74 policies that were surrendered, nine belonged to Aviva Directors.

(4) The cumulative impact of the failings represented a significant risk to the FSA objective of reducing financial crime.

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

(1) re-instating the value of any policies fraudulently surrendered;

(2) cooperating with other agencies, including supporting the police to assist them in identifying and arresting the criminals concerned;

(3) conducting an internal review to identify incidents of fraud and appointing a third party to carry out a review of Norwich Union Life's response to the fraud incidents and to review further the adequacy of caller identification procedures; and

(4) improving its anti-fraud procedures following that review.

2.9. Norwich Union Life has also co-operated fully with the FSA in the course of its investigation.

3. RELEVANT STATUTORY PROVISIONS

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

3.2. Under section 2(2) of the Act the reduction of financial crime is a regulatory objective for the FSA.

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

3.4. 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".

4. FACTS AND MATTERS RELIED ON

Background

4.1. Norwich Union Life, together with a number of other companies, is a business unit of the Aviva group of companies (Aviva Group). Each of these firms is authorised by the FSA. The ultimate parent company of these firms is Norwich Union Life Holdings Limited, which is a subsidiary of Aviva Group Holdings Limited, which in turn is owned by Aviva Plc. Norwich Union Life is one of the UK's largest life insurance businesses with in excess of seven million customers.

4.2. Norwich Union Life products include investment bonds, endowments savings plans and pension products. These products are all "life policies", designed for medium to long term savings and investments. Investment policies are capable of being surrendered at the request of the customer.

4.3. Norwich Union Life operates a number of call centres through which customers can obtain valuations of their policies, request amendments to their records (such as notifying changes of address or bank account details) and, in some circumstances, request an early surrender of their policies.

Aviva Group Fraud Policy

4.4. In December 2004, in setting out its financial crime strategy and objectives for 2005, Aviva Group highlighted five fraud themes. Identity theft and organised crime featured as two of those five themes (and were also highlighted as key drivers of fraud). Fraudulent surrenders of life insurance were also given as a recent example of fraud.

4.5. Throughout the Relevant Period, Aviva Group maintained a high level Group Fraud Policy. In addition to its Group Fraud Policy, Aviva Group introduced its Group Fraud Standards in October 2005 which contained nine group principles with which business units were required to comply. These group principles identified eight categories of fraud, including third party fraud (fraud perpetrated by individuals or entities unrelated to Aviva) and organised crime fraud (planned fraud committed systematically by a group of individuals against Aviva or the insurance industry).

4.6. From October 2005, Norwich Union Life was required to have in place procedures and controls that complied with the Group Fraud Policy and the Group Fraud Standards. This required Norwich Union Life to:

(1) undertake a fraud risk assessment to identify those areas susceptible to fraud and introduce preventative controls into new and existing systems and processes; and

(2) establish a fraud response plan that detailed how fraud will be reported and investigated within Norwich Union Life.

Norwich Union Life's relevant systems and controls

Caller identification procedures

4.7. Norwich Union Life operated a procedure to verify the identity of persons contacting Norwich Union Life call centres. These caller identification procedures were known within Norwich Union Life as "DPA checks", so called because they were originally designed for the purpose of compliance with the Data Protection Act 1998.

4.8. During the Relevant Period the caller identification procedures required callers to provide the following five pieces of information: surname, first and any middle names, first line of the address, date of birth and policy number.

4.9. If the caller did not pass the five initial checks, the caller identification procedures allowed call centre staff to select alternative questions from a secondary list of six questions: post code; policy type; policy term; bank details; mortgage provider or premium amount and method of payment. The post code was the first question in the secondary list.

4.10. Accordingly, callers could pass the caller identification procedures in the Relevant Period without quoting a valid policy number by correctly providing the following information: surname, first and any middle names, date of birth, first line of the address and postcode. All of this information can be acquired from publicly available sources.

Accessing customer information and amending records

4.11. Once the caller identification procedures were satisfied, Norwich Union Life procedures allowed callers to request and obtain further information, including the policy number, the value of the policy or their bank account details recorded by Norwich Union Life. Callers could also request changes to the details held by Norwich Union Life including for example the customer's address and the recorded bank account details.

4.12. Until November 2006, no additional checks were carried out by Norwich Union Life before it amended its record of a customer's address. Following notification of a change of address, Norwich Union Life procedure was to write to the new address to confirm that it had amended its records. However, it did not send a similar letter to the previous address.

Fraud suspicion procedures

4.13. Historically, Norwich Union Life had previously been subject to a limited number of policyholder and third party frauds, primarily arising from attempts by one party to cash in policies held jointly with a spouse. Compliance was responsible for the investigation of policyholder and third party fraud.

4.14. In circumstances where call handlers became suspicious of a caller, Norwich Union Life's procedure required the call handler to refer his suspicion by email to Norwich Union Life's fraud team (which was part of Compliance). The fraud team would normally act on the reported suspicion within 24 hours and, where appropriate, put a flag on the customer's record to indicate that an investigation was underway. In the meantime, neither the call handler's suspicions nor the fact that it had been reported to the fraud team was recorded on the customer's electronic record.

4.15. Further, call handlers were not always aware if there had been any recent amendments to a customer's electronic records or if a number of calls had recently been received. Call handlers would only be aware of any recent activity if they checked any notes made by previous call handlers on the customer's electronic records. Before August 2006, it was not standard practice to check the records before speaking to the caller. In August 2006 Norwich Union Life issued guidance to call handlers encouraging them to review the previous call history.

Monitoring and review of adequacy of controls

4.16. Following the introduction of the Group Fraud Standards in October 2005, Norwich Union Life was obliged to assess its anti-fraud systems and controls against the Group Fraud Standards. Norwich Union Life carried out a review of its anti-fraud systems and controls in April 2006 to assess whether those procedures complied with the principles in the Group Fraud Standards. However, its assessment of fraud controls did not include a review of the adequacy or effectiveness of the caller identification procedures as Norwich Union Life considered that the purpose of the DPA checks was to ensure that the business complied with the Data Protection Act 1998 rather than to act as part of Norwich Union Life's anti-fraud systems and controls.

4.17. Following the publication of an FSA Enforcement action in March 2006 concerning another regulated firm, Compliance assessed Norwich Union Life's financial crime controls and identified similar weaknesses both in Norwich Union Life's caller identification procedures and in its change of address procedures. Despite identifying the weaknesses, Norwich Union Life failed to act at the time to correct them. Remedial action in respect of these weaknesses was not taken until September and November 2006.

Customer impersonation incidents against Norwich Union Life

4.18. Beginning in April 2006, Norwich Union Life was the target of an organised fraud in which telephone callers, using information obtained from public sources such as Companies House, contacted Norwich Union Life call centres pretending to be genuine Norwich Union Life customers. By providing a customer's full name, address, postcode and date of birth, callers were able to satisfy the caller identification procedures and obtain access to customer information, including policy numbers and bank details.

4.19. Using this information, callers were able through a series of calls to request amendments to Norwich Union Life records, including changing the addresses and bank account details recorded for those customers. Falsified written surrender requests were submitted and in 74 cases funds were paid out to accounts controlled by the fraudsters.

4.20. The frauds were committed through a series of calls, often carried out in quick succession. For example, in the case of one policy, five calls were received by Norwich Union Life in one day. In another case three calls were received in 12 minutes. Even if call handlers had been suspicious and reported these matters to Norwich Union Life’s fraud team, the fraud team (whose normal response time was 24 hours) might not have responded in time. Further, as the call handlers did not record the suspicion report on the customer records and as call handlers differed from call to call, when a fraudster rang back the next call handler was unaware that a series of calls was being made.

4.21. Norwich Union Life was subject to 74 successful frauds, with a value of approximately £3.3 million. Attempts were made to obtain fraudulent surrenders in a further 558 cases. Confidential customer information relating to the policies was released in almost all of these 632 cases. In some cases, this included the customer's full bank account details.

Norwich Union Life's response to the frauds

4.22. Norwich Union Life first became aware that these frauds were taking place in April 2006 when fraudsters attempted to surrender the policy of a former director of an Aviva company.

4.23. In May 2006, Compliance investigated this attempted fraud and highlighted a number of weaknesses in Norwich Union Life’s procedures, including weaknesses in the caller identification procedures. Compliance made a recommendation that callers be required to provide their policy number in order to pass the caller identification procedures. This recommendation was not accepted by Norwich Union Life at the time on the grounds that it would impact on its levels of customer service and lead to customer dissatisfaction.

4.24. Compliance also recommended that following any change of address, Norwich Union Life should write to both the old and new addresses to confirm that it had amended its records. This recommendation was considered and investigated but was not acted on at the time because it would have required the introduction of a manual process to an otherwise automated procedure. A decision to implement such changes was made in October 2006.

4.25. This failure to act in an appropriate and timely manner to the frauds arose in part from a lack of clarity within Norwich Union Life regarding responsibility for the resolution of this issue. Norwich Union Life's procedures were insufficiently clear as to who was responsible for the management of its response to these actual and attempted frauds. As a result, Norwich Union Life did not give appropriate priority to the financial crime risks when considering those risks against competing priorities such as customer service.

4.26. By the end of July 2006 Norwich Union Life knew that the criminals' methodology used publicly available information - such as names, addresses and dates of birth available from Companies House records - to satisfy the caller identification procedures. Despite this, the business did not change the caller identification procedures. Instead, call centre staff were reminded to apply the existing caller identification procedures on every call.

4.27. Further, by the end of July 2006 more frauds had come to light and Norwich Union Life identified that customers affected included a number of current and former directors of Norwich Union Life and the wider Aviva Group (Aviva Directors). It was also aware that the frauds were not limited to policies held by Aviva Directors. Norwich Union Life's immediate response to the initial frauds focussed on the risks posed to policyholders who were Aviva Directors rather than on the risks posed to all of its customers. It took action to ensure that:

(1) it identified all Aviva Directors holding policies with Norwich Union Life and whose home address and personal information were in the public domain;

(2) all future communications to call centres in respect of these policies were highlighted for review by the fraud team for secondary approval;

(3) payments pending in respect of these policies were placed on hold pending further investigation; and

(4) call handlers reviewed a comments box on the call centre systems for warning notes and followed the instructions there carefully.

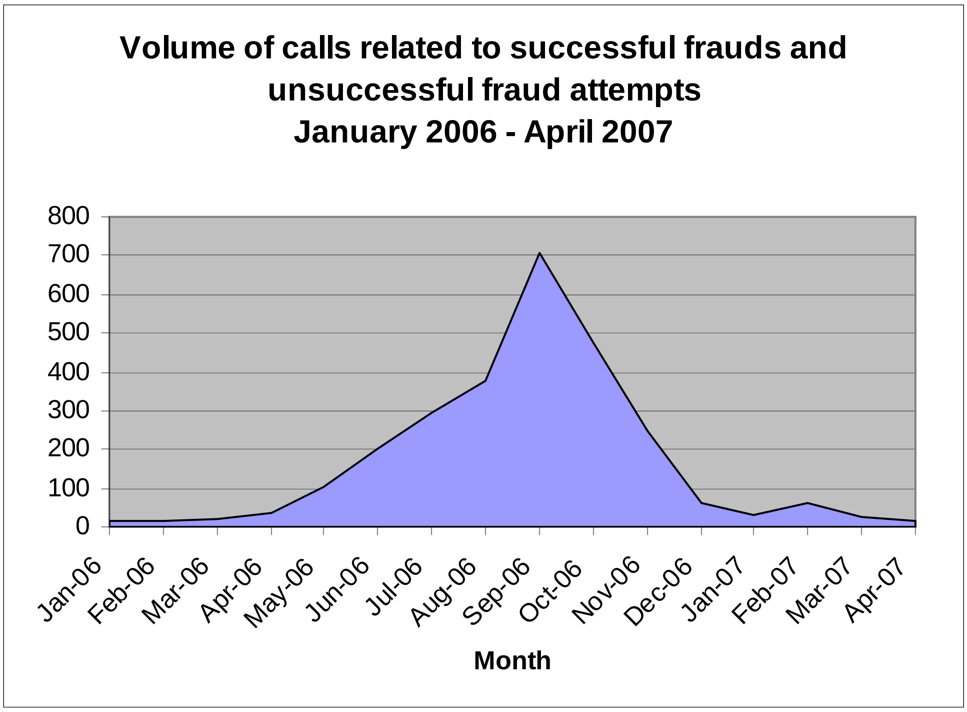
4.28. Of the 74 policies that were surrendered to the fraudsters over the course of the Relevant Period, nine belonged to Aviva Directors.

4.29. Norwich Union Life took action to protect all of its customers in September 2006 when call centre procedures were amended so that no change of address instruction could be made over the phone unless the caller could provide a valid policy number.

This action was made ineffective by the fact that callers could pass the caller identification procedures in one call, request and be provided with their policy number over the telephone, and then call back with the policy number to request a change of address.

4.30. Procedures were further amended in November 2006 so that neither policy numbers could be disclosed over the phone (callers were notified by post only) nor could full bank account details. In the same month a list of "Identity Theft Fraud Indicators" was circulated to the relevant Norwich Union Life administration teams to assist in the identification of fraud attempts.

4.31. The impact of these changes to the number of calls relating to incidents of fraud over time can be illustrated by reference to the following graph.



4.32. Norwich Union Life also worked closely with the police and other agencies in respect of the frauds, resulting in a number of arrests and the recovery of substantial sums defrauded from Norwich Union Life and its customers.

Principle 3 Breach - Systems and Controls

4.33. By reason of the facts and matters set out above, the FSA considers that Norwich Union Life has contravened Principle 3 of the FSA's Principles for Business, namely that Norwich Union Life failed to take reasonable care to:

(1) assess where its financial crime risks lay and establish adequate procedures and controls to manage those risks; and

(2) respond to the frauds in an appropriate and timely manner once they had become apparent.

Caller identification procedures

4.34. The FSA views Norwich Union Life's conduct as particularly serious because Aviva Group highlighted the risks of fraudulent investment surrenders through identity theft as early as December 2004. Norwich Union Life should have considered financial crime risk across its business and assessed the controls in place to ensure that they remained appropriate to withstand new and emerging risks to the business (such as customer impersonation and identity theft).

4.35. However, during the Relevant Period Norwich Union Life's caller identification procedures were inadequate in that callers could use publicly available information to pass them. Once past the caller identification procedures, criminals could and did obtain confidential information including bank account details, change customer records and request the surrender of policies.

Response to the discovery of the frauds

4.36. Norwich Union Life failed to take reasonable care to ensure that it had effective systems and controls in place to enable it to respond in an appropriate and timely manner to the frauds. As a result, the defects in the caller identification procedures were allowed to remain in place for a significant period of time after Norwich Union Life became aware of the methodology being used by the fraudsters. Whilst steps to prevent further release of customer information and/or funds were identified by Compliance shortly after discovery of the first successful frauds, those steps were not implemented in a timely manner.

4.37. Norwich Union Life took appropriate action to protect the Aviva Directors who it initially identified as being specifically targeted by the fraudsters, but it took inadequate steps to assess the risk to customers generally. This is despite the fact that it knew that the fraudsters were using Companies House details to overcome their caller identification checks by the end of July 2006. This failure to take adequate and timely steps to investigate the extent to which customers were exposed increased the risk of further financial crime.

5. FACTORS RELEVANT TO DETERMINING THE PROPOSED 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 the FSA's Decision Procedure and Penalties Manual (DEPP) which forms part of the FSA Handbook. DEPP 6.5 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.

DEPP 6.5.1 G states that the criteria listed in DEPP 6.5 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 Norwich Union Life'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 affected. The FSA has also had regard to the value of the fraudulent surrenders. 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. The risk of loss to customers in this case is particularly high given the number of Norwich Union Life customers, the weaknesses in the caller verification checks in place and the additional information that could be obtained having passed those checks.

5.4. The FSA considers that the fact that the control failures resulted in the surrender of policies to fraudsters is an aggravating feature of this case, but this is not the sole reason for imposing a penalty. The defects in the procedures alone are a cause of significant concern and exposed Norwich Union Life's customers to the risk of financial crime. The FSA recognises that Norwich Union Life reinstated all fraudulently surrendered policies.

5.5. Throughout the Relevant Period Norwich Union Life did not take adequate care to consider the risks of customer impersonation. The FSA requires firms to undertake a risk-based assessment of financial crime risk and where necessary to implement controls to mitigate the risk.

5.6. 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 financial crime 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 failures by the firm arose during this period of heightened awareness of financial crime issues. Throughout the Relevant Period Norwich Union Life was aware of the increasing risk of identity theft.

5.7. The FSA considers it particularly serious that the failures by the firm continued even after the nature of the criminals' methodology was known and following warnings given by Compliance in May and July 2006, that its controls were not wholly adequate.

5.8. The FSA has had regard to the size, financial resources and other circumstances of Norwich Union Life. Norwich Union Life is the one of the largest life insurance businesses in the UK.

5.9. Details of Norwich Union Life's response to the frauds are set out above. The FSA considers the firm's failure to address the risk in a timely and appropriate way arising from the ongoing frauds to be a serious failure.

5.10. Norwich Union Life has taken the following steps to address the risks to customers:

(1) Policy numbers are not given out over the phone;

(2) Bank details are not given out over the phone;

(3) Change of address instructions can only be accepted over the phone if the policy number is provided by the caller;

(4) Notification of change of address is sent to old and new addresses;

(5) Contact centre staff and surrender administration teams have been issued with revised guidance with fraud indicators highlighted.

5.11. Throughout the FSA's investigation, Norwich Union Life has co-operated fully and worked with the FSA. Norwich Union Life has also cooperated with police enquiries into the frauds.

5.12. The FSA has had regard to previous cases involving breaches of system and control requirements that threaten the FSA's financial crime objective. Norwich Union Life has not been the subject of FSA enforcement action previously.

6. DECISION MAKER

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

7. IMPORTANT

7.1. This Decision Notice is given to you 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 Norwich Union Life to the FSA by no later than 31 December 2007, 14 days from the date of the Final Notice.

If the financial penalty is not paid

7.3. If all or any of the financial penalty is outstanding on 1 January 2008, the FSA may recover the outstanding amount as a debt owed by Norwich Union Life 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.

FSA contacts

For more information concerning this matter generally, you should contact Mark Lewis of the Enforcement Division of the FSA (direct line: 020 7066 4244/fax: 020 7066 4245).

…………………………………………….

Tracey McDermott
FSA Enforcement Division