Control failure

Norwich Union Life knew that its weak identity controls exposed customers to fraud, but didn't do enough about it. The result? A record fine from the Financial Services Authority, as Neil Hodge reports

IN DECEMBER THE UK'S financial services regulator the Financial Services Authority (FSA) fined insurance firm Norwich Union Life – one of the UK's largest life insurers – £1.26m, a record amount for an information security breach. The regulator said the firm did not have effective systems and controls in place to protect customers' confidential information and manage its financial crime risks, despite repeated warnings by the insurer's compliance function that controls were inadequate.

The weaknesses in Norwich Union Life's systems and controls allowed fraudsters to use publicly available information, including names, addresses and dates of birth, to impersonate customers and obtain sensitive customer details from its call centres. Once through the customer vetting process, the fraudsters were then able (in some cases) to ask for confidential customer records, including addresses and bank account details, to be altered. The fraudsters used this information to request the surrender of 74 customers' policies totalling £3.3m.

Over 632 policies were targeted by the fraudsters in total and, regardless of whether a policy was surrendered or not, confidential customer information was disclosed in almost all cases. Yet the insurer only decided to act when nine policies belonging to current and former directors of the Aviva group – Norwich Union Life's parent company – were targeted, despite evidence that other policyholders were also at risk.

Failure to act

During its investigation, the FSA found that Norwich Union Life had failed to properly assess the risks posed to its business by financial crime, particularly customers' personal information, even after these risks had been identified by its own compliance department on a number of occasions. Remedial action in respect of these weaknesses was not taken until September and November 2006. As a result, its customers were more likely to fall victim to financial crimes such as identity theft, said the regulator.

"Over 632 policies were targeted by the fraudsters in total and confidential customer information was disclosed in almost all cases"

The FSA said that Norwich Union Life breached Principle 3 of the regulator's "Principles for Business". This states that "a firm must take reasonable care to organise and control its affairs responsibly and effectively with adequate risk management systems". It said the firm failed 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.

Crack down

One lawyer believes that the FSA's harsh criticism of Norwich Union Life's conduct signifies a tougher stance by the regulator, particularly regarding data protection. Nathan Willmott, partner in the financial services and markets group at law firm Berwin Leighton Paisner, says that "the FSA is cracking down a lot harder on any incident that involves the lack of security surrounding customer data. The regulator has flagged data protection as a key issue for financial services firms for several years, so any security breach will be seen as a major failure in controls and consumer confidence – particularly when it happens in one of the UK's largest insurers."

In the last two years, the FSA has fined BNPP Private Bank £350,000, Nationwide £980,000 and Capita Financial Administrators £300,000 for failings relating to information security lapses and fraud.

Norwich Union Life's troubles began in April 2006 when it discovered that it was the target of an organised fraud in which telephone callers, using publicly available personal information such as names, addresses and dates of birth from Companies House, contacted the insurer's call centres pretending to be genuine customers.

Lax controls meant that by providing a customer's full name, address, postcode and date of birth, callers were able to satisfy the caller identification procedures then in place and obtain access to customer information, including policy numbers and bank details. Using that information, callers were then able to request amendments to customer records, including changing their addresses and bank account details.

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. Yet nothing was flagged up.

The insurer only became aware that these frauds were taking place in April, when fraudsters attempted to surrender the policy of a former director of an Aviva company. The following month, the compliance function investigated this attempted fraud and highlighted a number of weaknesses in the insurer's procedures, including weaknesses in the caller identification procedures. However, nothing was done about it, said the FSA.

By the end of July 2006 Norwich Union Life knew that criminals were using publicly available information to circumvent its controls. Despite this, the business did not change the caller identification procedures. Instead, call centre staff were reminded to apply the existing rules on every call.

Furthermore, more frauds had come to light, but the insurer's immediate response focussed on the risks posed to policyholders who were former or current Aviva directors rather than on the risks posed to all of its customers (only nine of the 74 policies that were surrendered to fraudsters belonged to Aviva directors). Such an attitude did not impress the regulator.

Flawed checks

At the time, Norwich Union Life operated a procedure to verify the identity of persons contacting its call centres known as "DPA checks", so called because they were originally designed for the purpose of compliance with the Data Protection Act 1998. The insurer's caller identification procedures required callers to provide their surname, first and any middle names, first line of the address, date of birth and policy number. 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, such as 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. That meant callers could pass the caller identification procedures without quoting a valid policy number just by correctly providing personal details – all of which can be acquired from publicly available sources.

"The FSA is cracking down a lot harder on any incident that involves the lack of security surrounding customer data"

Lessons to be learnt

Experts spell out their top-tips for companies and internal auditors to follow:

1. **Ensure the company fully understands the regulatory and legal requirements,** says Gary Dixon, managing director of professional services firm Resources Compliance – in this case, the FSA guidelines and the Data Protection Act.
2. **Ensure that all staff understand their responsibilities and the implications,** Dixon says that financial services companies have higher control demands placed upon them as a result of the higher impact of a breach in systems. For regulated companies, such as Norwich Union Life, this means that not only will the company be at risk of a fine, but also the managers and directors responsible are personally at risk of fine, censure or even imprisonment in extreme cases,
3. **Phase out the reliance on publicly-available data.** Paul Williams, chair of the ISACA strategic advisory group and IT governance adviser at risk management consultancy Protiviti, says that reliance on publicly available data is totally inappropriate to safeguard against threats such as identity theft. Organisations should consider using less available yet equally memorable information, such as the registration number or make of the first car owned, or the name of a childhood best friend.
4. **Apply very strict rules on requests to change data or initiate transactions over the phone.** All sensitive changes need to be confirmed with additional evidence, says Williams, such as the provision of utility bills to support an address change or a request for a written, signed, notification to support a bank account change. Such changes should never be accepted just on the basis of a telephone call.
5. **Don't forget to protect information in the internal audit,** compliance or fraud departments. Andrew Durant, managing director in professional services firm Navigant Consulting's European disputes and investig.ations practice, points out that the Norwich Union Life fraudsters appeared to know where the system was weak and abused it. "Knowledge about how to work the control system is just as dangerous in the wrong hands as the customer data such controls are designed to protect," he says. However, there was no suggestion of any leak in this case.

Let down

"Norwich Union Life let down its customers by not taking reasonable steps to keep their personal and financial information safe and secure," said **Margaret Cole**, director of enforcement at the Financial Services Authority. "It is vital that firms have robust systems and controls in place to make sure that customers' details do not fall into the wrong hands. Firms must also frequently review their controls to tackle the growing threat of identity theft."

"This fine is a clear message that the FSA takes information security seriously and requires that firms do so too," she added.

Mark Hodges, chief executive of Norwich Union Life, said: "We are sorry that this situation arose and apologised to the affected customers when this happened. We have extensive procedures in place to protect our customers but in this instance weaknesses were exploited and we were the target of organised fraud."

The insurer agreed to settle at the early stage of the FSA's investigation and qualified for a 30% discount under the FSA's executive settlement procedure. Without the discount, the fine would have been £1.8m.

Once these caller identification procedures were satisfied, callers could 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 the insurer, including the customer's address and the recorded bank account details. Until November 2006, no additional checks were carried out.

In circumstances where call handlers became suspicious of a caller, procedure required the call handler to refer his suspicion by email to the insurer's fraud team, which 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. However, 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. Furthermore, 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. They 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.

Poor assessment

Norwich Union Life had implemented a group-wide fraud standard in October 2005 and a review of its anti-fraud systems and controls was carried out in April 2006. However, its assessment did not include a review of the adequacy or effectiveness of the caller identification procedures. This was because Norwich Union Life considered that the purpose of the DPA checks was to ensure that the business complied with the Data Protection Act rather than to act as part of its own anti-fraud systems and controls.

While compliance staff made a recommendation that callers be required to provide their policy number in order to pass the caller identification procedures, this was not accepted at the time on the grounds that it would impact on its levels of customer service and lead to customer dissatisfaction. The function also recommended that following any change of address, the insurer should write to both the old and new addresses to confirm that it had amended its records. This recommendation was considered but was not acted on because it would have required the introduction of a manual process to an otherwise automated procedure. A decision to implement such changes was not made until October 2006.

"'Norwich Union Life's procedures were insufficiently clear as to who was responsible for the management of its response to these frauds,' said the FSA"

The FSA said that "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". Furthermore, "Norwich Union Life's procedures were insufficiently clear as to who was responsible for the management of its response to these frauds," said the FSA. "As a result, the insurer did not give appropriate priority to the financial crime risks when considering those risks against competing priorities such as customer service." □