CyTRAP Labs GmbH

Roentgenstrasse 49 Street
CH-8005 Zuerich Zip Code
Switzerland Country

+41(0)44 272 1876 Voice
+41(0)76 200 7778 Cell

www.CyTRAP.eu URL
info@CyTRAP.eu E-Mail

See also

UK - FSA fines Norwich Union Life £1.26m for exposing its customers to the risk of fraud (choose option Login as Guest – click on this link again = free access)

More information about these issues particularly fines in the UK regarding risk and information security management that fails to meet standards you can find here:

UK - more fines for lack of compliance, risk management and information security (choose option Login as Guest – click on this link again = free access)

For other countries see also:

CyTRAP labs glossary - The judge says - war stories - PR disasters *(choose option Login as Guest – click on this link again = free access)*

3 data security breach regulation - soon we should be able to make a business case for security

T

http://www.fsa.gov.uk/pages/Library/Communication/PR/2007/130.shtml

FSA fines Norwich Union Life £1.26m for exposing its customers to the risk of fraud

“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. ”

FSA/PN/130/2007
17 December 2007

The Financial Services Authority (FSA) has fined Norwich Union Life £1.26 million for not having effective systems and controls in place to protect customers' confidential information and manage its financial crime risks. These failings resulted in a number of actual and attempted frauds against Norwich Union Life's customers.

The weaknesses in Norwich Union Life's systems and controls allowed fraudsters to use publicly available information including names and dates of birth to impersonate customers and obtain sensitive customer details from its call centres. They were also, in some cases able to ask for confidential customer records such as addresses and bank account details to be altered. The fraudsters then used the information to request the surrender of 74 customers' policies totalling £3.3 million in 2006.

During its investigation, the FSA found that Norwich Union Life had failed to properly assess the risks posed to its business by financial crime, including fraudsters seeking to obtain customers' confidential information. As a result, its customers were more likely to fall victim to financial crimes such as identity theft.

Margaret Cole, director of enforcement, said:

"Norwich Union Life let down its customers by not taking reasonable steps to keep their personal and financial information safe and secure.

CyTRAP Labs GmbH

"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."

Norwich Union Life also failed to address the issues, highlighted by the frauds, in an appropriate and timely manner even after they were identified by its own compliance department. The failings happened at a time of increasing awareness across the UK about the importance of information security.

Norwich Union Life co-operated fully with the FSA in the course of the investigation. It has taken a number of remedial actions including co-operating with the police to identify and arrest the fraudsters and carrying out a review of its information security processes. Norwich Union has reinstated all fraudulently surrendered policies in full.

Norwich Union Life 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 £1.8 million.

Notes for editors

1. Norwich Union Life is one of the UK's largest life insurance businesses with 6.8 million customers in the UK.
2. The full text of the Final Notice issued by the FSA, includes the background to the case, the relevant statutory provisions, regulatory requirements contravened, and the factors taken into account when setting the level of the fine.
3. 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.
4. FSA Principle 3 states that a firm must take reasonable care to organise and control its affairs responsibly and effectively, with adequate risk management systems.
5. In November 2004 the FSA published a report entitled 'Countering Financial Crime Risks in Information Security'. 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 addition, the FSA is currently carrying out a major project examining the systems and controls used by a range of financial services firms to protect their customers' data; the findings from this work will be published in 2008.
6. The FSA regulates the financial services industry and has four objectives under the Financial Services and Markets Act 2000: maintaining market confidence; promoting public

understanding of the financial system; securing the appropriate degree of protection for consumers; and fighting financial crime.

7. The FSA aims to promote efficient, orderly and fair markets, help retail consumers achieve a fair deal and improve its business capability and effectiveness.

http://www.fsa.gov.uk/pages/Library/Communication/PR/2007/060.shtml

FSA fines BNPP Private Bank £350,000 for weak anti-fraud controls

"This is a warning to other firms that we are raising our game in this area and expect them to follow suit. "

FSA/PN/060/2007
10 May 2007

The Financial Services Authority (FSA) has today fined BNP Paribas Private Bank (BNPP Private Bank) £350,000 for weaknesses in its systems and controls which allowed a senior employee to fraudulently transfer £1.4 million out of clients' accounts without permission.

This is the first time a private bank has been fined for weaknesses in its anti-fraud systems. The 13 fraudulent transactions were carried out between February 2002 and March 2005 using forged clients' signatures and instructions and by falsifying change of address documents.

During its investigation, the FSA found that BNPP Private Bank did not have an effective review process for large transactions, over £10,000, from clients' accounts. It also found that the bank's procedures were not clear about the role of senior management in checking significant transfers prior to payment. As a result, a number of fraudulent transactions were not independently checked. In addition, a flaw in the bank's IT system allowed the senior employee to evade the normal Middle Office processes. This meant that basic authorisation and signatory checks were not carried out on internal cash transfers between different customer accounts.

Margaret Cole, FSA Director of Enforcement, said:

"BNPP Private Bank's failures exposed clients' accounts to the risk of fraud. This is unacceptable particularly with the overall increase in awareness around fraud and client money risks. Senior management must make sure their firms have robust systems and controls to reduce the risk of them being used to commit financial crime.

"This is a warning to other firms that we are raising our game in this area and expect them to follow suit. We will not hesitate to take action against any firm found wanting."

BNPP Private Bank's failings were serious because they enabled significant fraud to take place and failed to detect subsequent transfers to cover it up for a long period of time. The bank also failed to improve its procedures for monitoring large transactions or carry out remedial action on a timely basis. This was despite the bank being aware that certain of its procedures required improvement as a result of an FSA visit in relation to money laundering systems and controls in August 2002 and subsequent internal reviews.

The FSA recognises that BNPP Private Bank has since taken steps to correct the failings and no customers suffered loss. Also, a subsequent independent review of the bank's anti–fraud systems and controls found them to have no significant weaknesses. The bank brought the fraud to the FSA's attention and has co-operated fully with the investigation. BNPP Private Bank qualified for a 30% discount under the FSA's executive settlement procedures by agreeing to settle at an early stage of the investigation.

Notes to editors

1. In the last two years, the FSA has fined Nationwide, Capita Group and Kyte for weaknesses in their anti fraud systems and controls.
2. BNPP Private Bank is an EEA passported firm based in London. It is wholly owned by BNPP SA France and its subsidiaries "the BNPP Group".
3. The full text of the Final Notice issued by the FSA, which includes the background to the case, the relevant statutory provisions, regulatory requirements contravened, and the factors taken into account when setting the level of the fine can be found on the website.
4. FSA Principle 3 states that a firm must take reasonable care to organise and control its affairs responsibly and effectively, with adequate risk management systems.
5. In his speech at the Financial Crime conference in January, John Tiner, FSA chief executive announced the creation of a new Financial Crime and Intelligence Division (FCID). The FCID brings together all of the financial crime expertise that was previously spread throughout the FSA and will work closely with others to identify, assess and manage criminal threats in the UK's financial sector.
6. The FSA regulates the financial services industry and has four objectives under the Financial Services and Markets Act 2000: maintaining market confidence; promoting public understanding of the financial system; securing the appropriate degree of protection for consumers; and fighting financial crime.
7. The FSA aims to promote efficient, orderly and fair markets, help retail consumers achieve a fair deal and improve its business capability and effectiveness.

CyTRAP Labs GmbH

http://www.fsa.gov.uk/pages/Library/Communication/PR/2007/021.shtml

FSA fines Nationwide £980,000 for information security lapses

"The FSA took swift enforcement action in this case to send a clear, strong message to all firms about the importance of information security."

FSA/PN/021/2007
14 February 2007

The Financial Services Authority (FSA) has today fined Nationwide Building Society (Nationwide) £980,000 for failing to have effective systems and controls to manage its information security risks. The failings came to light following the theft of a laptop from a Nationwide employee's home last year.

During its investigation, the FSA found that the building society did not have adequate information security procedures and controls in place, potentially exposing its customers to an increased risk of financial crime.

The FSA also discovered that Nationwide was not aware that the laptop contained confidential customer information and did not start an investigation until three weeks after the theft.

Nationwide's failings occurred at a time of heightened awareness of information security issues as a result of government initiatives, increasing media coverage and an FSA campaign about the importance of information security.

Margaret Cole, director of enforcement, said:

"Nationwide is the UK's largest building society and holds confidential information for over 11 million customers. Nationwide's customers were entitled to rely upon it to take reasonable steps to make sure their personal information was secure.

CyTRAP Labs GmbH

"Firms' internal controls are fundamental in ensuring customers' details remain as secure as they can be and, as technology evolves, firms must keep their systems and controls up-to-date to prevent lapses in security.

"The FSA took swift enforcement action in this case to send a clear, strong message to all firms about the importance of information security."

The FSA acknowledges that Nationwide has co-operated fully in the course of the investigation and has undertaken a number of actions to address this failure, including: taking a range of additional measures to increase security around accounts; informing customers of the loss of information; affirming its existing policy to reimburse any customer that has suffered financial loss as a result of this incident; and commissioning a comprehensive review of its information security procedures and controls.

By agreeing to settle at an early stage of the FSA's investigation Nationwide qualified for a 30% discount under the FSA's executive settlement procedures – without the discount the fine would have been £1.4 million.

Notes for editors

1. The full text of the Final Notice issued by the FSA, which includes the background to the case, the relevant statutory provisions, regulatory requirements contravened, and the factors taken into account when setting the level of the fine may be found on the website.
2. FSA Principle 3 states that a firm must take reasonable care to organise and control its affairs responsibly and effectively, with adequate risk management systems.
3. In November 2004 the FSA published a report entitled 'Countering Financial Crime Risks in Information Security'. 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.
4. The FSA regulates the financial services industry and has four objectives under the Financial Services and Markets Act 2000: maintaining market confidence; promoting public understanding of the financial system; securing the appropriate degree of protection for consumers; and fighting financial crime.
5. The FSA aims to promote efficient, orderly and fair markets, help retail consumers achieve a fair deal and improve its business capability and effectiveness.

http://www.fsa.gov.uk/pages/Library/Communication/PR/2006/019.shtml

FSA fines Capita Financial Administrators Limited £300,000 in first anti-fraud controls case

"With fraud becoming an increasing menace, firms must fully understand the risks they face and have robust anti-fraud controls in place. "

FSA/PN/019/2006
16 March 2006

The FSA has fined Capita Financial Administrators Limited (CFA), a third party administrator of collective investment schemes, £300,000 for poor anti-fraud controls over client identities and accounts.

The FSA found that CFA had inadequately considered the risks posed by fraud and had not maintained effective systems and controls to mitigate the risk of fraud. This is the first time the FSA has fined a firm for failures of anti-fraud systems and controls.

The failures in controls contributed to a small number of significant actual and attempted frauds against the firm's customers. These appear to have been facilitated by colluding CFA staff. The initial frauds were not discovered by CFA but instead were brought to the firm's attention by clients.

Philip Robinson, Financial Crime Sector leader said:

"With fraud becoming an increasing menace, firms must fully understand the risks they face and have robust anti-fraud controls in place.

"The nature of CFA's business, because it holds information on client identity, makes it particularly vulnerable to fraud. Yet the firm failed to adequately consider this risk in the business.

CyTRAP Labs GmbH

"Our recent report on fraud governance found that parts of the financial services industry can do more to protect themselves and this case demonstrates that we take a firm's failures seriously."

CFA is a third party administrator that is responsible for carrying out client instructions to buy and sell investments. In August 2004, CFA discovered that a client's name and address had been changed and the sale of units was being processed without instructions from the client. The firm then found that the data for five other clients had been subject to unauthorised changes. Fraudulent requests for payments totalling £1,134,938 had been made but were stopped from going ahead by CFA.

In September and December 2004, CFA discovered further actual and attempted frauds, including instructions for £417,321 being processed for 20 clients. Actual fraudulent payments totalling £328,241 were made.

The weaknesses in systems and controls contributed to the frauds. There were insufficient controls to ensure that changes to client data and instructions for payments were genuine or that payments were not made to accounts that were not controlled by clients. CFA did not ensure that procedures to mitigate fraud risk were adequately implemented and that fraud awareness training was appropriate.

Since the frauds were discovered, the Capita Group has put in place an effective remedial programme at CFA. It has taken a positive approach to improving systems and has implemented controls at CFA that are consistent with best practice in the industry. CFA also took prompt action to ensure that its clients did not suffer financial loss as a result of the frauds.

The matters set out in this notice refer to the actions of CFA and not the wider Capita Group.

Notes to editors

1. The full text of the final notice includes background to the case, the relevant statutory provisions and the regulatory requirements contravened.
2. CFA's penalty is in respect of breaches of Principle 2 and Principle 3 of the FSA's Principles for Businesses and breaches of Senior Management Arrangements, Systems and Controls SYSc 3.2.6R
3. On 27 February 2006, the FSA published its report on fraud governance in financial services firms (see press release 014/2006)
4. On 26 October 2004 Philip Robinson's speech set out the FSA's approach to fighting fraud in partnership.

5. The FSA regulates the financial services industry and has four objectives under the Financial Services and Markets Act 2000: maintaining market confidence; promoting public understanding of the financial system; securing the appropriate degree of protection for consumers; and fighting financial crime.
6. The FSA aims to promote efficient, orderly and fair markets, help retail consumers achieve a fair deal and improve its business capability and effectiveness.