

---

**FINAL NOTICE**

---

To: Merchant Securities Group Limited

Of: John Stow House  
18 Bevis Marks  
London  
EC3A 7JB

Date: 13 June 2008

**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 Merchant Securities Group Limited (Merchant Securities/the Firm) a Decision Notice on 12 June 2008 which notified Merchant Securities that pursuant to section 206 of the Financial Services and Markets Act 2000 (the Act), the FSA had decided to impose a financial penalty of £77,000 on Merchant Securities in respect of breaches of Principle 3 of the FSA's Principles for Businesses (Principle 3).
- 1.2. Merchant Securities 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 the FSA would have imposed a financial penalty of £110,000 on the Firm.

1.3. Merchant Securities had agreed that it will not be referring the matter to the Financial Services and Markets Tribunal.

1.4. Accordingly, for the reasons set out below and having agreed with Merchant Securities the facts and matters relied on, the FSA imposes a financial penalty on Merchant Securities in the amount of £77,000.

## **2. REASONS FOR THE ACTION**

2.1. Merchant Securities has breached Principle 3 with respect to its systems and controls in relation to financial crime, specifically the security of customer information. It has not taken reasonable care to organise and control its affairs responsibly and effectively, with adequate risk management systems. In particular, although there is no evidence of actual compromise of customer information, Merchant Securities has not taken reasonable care to establish and maintain effective systems and controls for countering the risk that customer information held by the Firm might be compromised by theft, loss or unauthorised alteration.

2.2. Specifically, prior to October 2007, Merchant Securities failed to:

(1) assess adequately the risks associated with its procedures for verifying the identity of its customers over the telephone and failed to implement adequate procedures. As a result, it exposed its customers to the risk of impersonation by fraudsters;

(2) assess and mitigate adequately the risk that customers' account access information could be intercepted or lost where such information was included in its written communications with its customers;

(3) assess and mitigate adequately the risk of unauthorised access to its back-up tapes during the times in which the tapes were stored outside office premises. This exposed customers to the risk that information stored on those tapes could be stolen or lost; and

- (4) implement adequate controls to mitigate the risk of customers' personal data being transmitted outside the Firm by failing to prevent the use of instant messaging and web-based email.
- 2.3. These failures increased the risk that Merchant Securities could be used for a purpose connected to financial crime.
- 2.4. Merchant Securities' failures adequately to assess the risks of data compromise and the impact this could have on its customers and its reputation occurred against a background of heightened public awareness of information security. Further, its failings occurred during a period in which the FSA published a series of Final Notices about regulatory action taken against firms for failures relating to information security in cases involving actual compromise of customer data.
- 2.5. Merchant Securities should therefore have been aware of the ways in which business practices can place customer information at risk and should have been aware that its own failings could have resulted in actual data compromise and customer detriment.
- 2.6. While there is no evidence of actual compromise of customer information, Merchant Securities' failures are serious and therefore merit enforcement action and the imposition of a financial penalty.

### **Relevant Statutory Provisions And Guidance**

- 2.7. 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.
- 2.8. Under section 2(2) of the Act the reduction of financial crime is a regulatory objective for the FSA.
- 2.9. The FSA's Principles for Businesses constitute requirements imposed on authorised persons under the Act.

2.10. Principle 3 states that:

*“A firm must take reasonable care to organise and control its affairs responsibly and effectively, with adequate risk management systems”.*

2.11. The FSA's Decision Procedure and Penalties Manual (DEPP) came into effect on 28 August 2007. The FSA has had regard to the relevant provisions in DEPP and, owing to the duration of Merchant Securities' breaches, has also had regard to the relevant guidance set out in the Enforcement Manual (ENF) which preceded DEPP.

## **FACTS AND MATTERS RELIED ON**

### **Background**

2.12. Merchant Securities is a stock-broking firm with approximately 850 retail and institutional customers whom it advises and for whom it arranges deals in investments. Its retail customers are predominantly high-net worth individuals.

2.13. 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, government initiatives have sought to increase awareness of the risks of identity theft, and media coverage of identity theft risks has been widespread.

2.14. Since March 2006 the FSA published several Final Notices about regulatory action taken against firms for failures to take reasonable care to ensure they had effective systems and controls to manage risks relating to information security and to counter the risks of being used to further financial crime. These Final Notices were published by the FSA on its website and attracted wide press and general interest.

2.15. During 2007 the FSA visited a number of firms as part of an ongoing programme of work on identifying and mitigating risks to the FSA's statutory financial crime objective. On 7 September 2007 the FSA visited Merchant Securities (the Thematic Visit). The purpose of the Thematic Visit was to gather information on how the Firm assessed and managed its data security risks and how it safeguarded customer data.

### **Breach of Principle 3**

- 2.16. A number of business practices identified during the Thematic Visit exposed customers to the risk that customer information held by the Firm might be compromised. In particular:
- (1) Merchant Securities procedure for identifying its customers when obtaining instructions by telephone, when considered in the light of the Firm's systems and controls as a whole, exposed its customers to the risk of impersonation by fraudsters. Advisors relied on recognising customers' voices to identify their clients and by talking with them informally about personal matters such as holidays or hobbies. However, each advisor had approximately 150 customers, of whom only 20% had frequent contact with the Firm;
  - (2) Customers' account numbers were included in the Firm's written communications (mail) with clients. It would have been possible for such mailings to have been intercepted. A fraudster in possession of the customer's name and the customer reference number could then access that customer's account information;
  - (3) Merchant Securities had no adequate procedure for the secure storage of back-up tapes. Back-up tapes, containing unencrypted personal client information, were stored overnight in a bag at the home of a member of staff; and
  - (4) Merchant Securities had no adequate procedure for controlling and monitoring the use of instant messaging and web-based email. A number of employees with access to relevant customer data on their computers were able to use instant messaging and web-based email. Monitoring for use of instant messaging and web-based email was ad-hoc and focused on productivity rather than information security. Web-based email presents a particular risk because its content cannot be monitored or retrieved by firms.
- 2.17. Merchant Securities should have been aware, particularly in light of recent FSA regulatory actions, that each of these practices in isolation was sufficient to place customer data at risk of loss, theft or alteration.

### **Analysis of Sanction**

2.18. In deciding upon the level of disciplinary sanction, regard has been had to all the relevant circumstances of the case and to the guidance set out in DEPP and ENF. The following are particularly relevant:

- (1) the need for the penalty imposed to act as a deterrent both to Merchant Securities and other firms;
- (2) the nature, seriousness and impact of the breach, including the risk of loss to consumers;
- (3) the size, financial resources and other circumstances of the Firm, including the Firm's trading update of 1 May 2008;
- (4) the Firm's failure to pay proper heed to the warning signals referred to in paragraphs 2.13 and 2.14 above; and
- (5) that the breaches were identified by the FSA rather than by Merchant Securities.

2.19. The FSA recognises that:

- (1) there is no evidence of any actual compromise of customer data; and
- (2) Merchant Securities has now taken steps to review and improve its systems and controls in relation to information security.

### **Conclusion**

2.20. From these facts and matters the FSA has determined that the Firm failed prior to October 2007 to assess adequately its controls or to implement and maintain controls which were adequate to mitigate the risk to its customers' information. The Firm should have been aware that its controls were inadequate. Merchant Securities' failings exposed its customers to the risk of data compromise.

### **3. DECISION MAKER**

- 3.1. The decision which gave rise to the obligation to give this notice was made by the Settlement Decision Makers on behalf of the FSA.

### **4. IMPORTANT**

- 4.1. This Final Notice is given to Merchant Securities in accordance with section 390 of the Act.

#### **Manner and time for Payment**

- 4.2. The FSA has agreed to allow the firm to pay the financial penalty in two instalments. The financial penalty must be paid by Merchant Securities to the FSA as follows: £40,000 by no later than 27 June 2008 and the remainder by 14 July 2008.

#### **If the Penalty is not paid**

- 4.3. If all or any of the financial penalty is outstanding on 14 July 2008, the FSA may recover the outstanding amount as a debt owed by Merchant Securities and due to the FSA.

#### **Publicity**

- 4.4. 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.
- 4.5. The FSA intends to publish such information about the matter to which this Final Notice relates as it considers appropriate.

**FSA contacts**

- 4.6. For more information concerning this matter generally, you should contact Dermot Lynch at the FSA (direct line: 020 7066 1206 /fax: 020 7066 1207).

**William Amos**

**FSA Enforcement Division**