Chapter 6

Data security in Financial Services (2008)

6.1 Introduction

6

6.1.1 **Who should read this chapter?** This chapter is relevant, and its statements of good and poor practice apply, to **all firms** subject to the financial crime rules in ■ SYSC 3.2.6R or ■ SYSC 6.1.1R and to **e-money institutions** and **payment institutions** within our supervisory scope.

6.1.2 In April 2008 the *FSA* published the findings of our thematic review on how financial services firms in the UK were addressing the risk that customer data may be lost or stolen and used to commit fraud or other financial crime. The *FSA* visited 39 firms, including retail and wholesale banks, investment firms, insurance companies, financial advisers and credit unions. The *FSA* also took into account our experience of data loss incidents dealt with by our Financial Crime Operations Team: during 2007, the team dealt with 56 cases of lost or stolen data from financial services firms.

6.1.3 The *FSA* found a wide variation between good practices demonstrated by firms that were committed to ensuring data security and weakness in firms that were not taking adequate steps. Overall, the *FSA* found that data security in financial services firms needed to be improved significantly.

6.1.4 The report concluded that poor data security was a serious, widespread and high-impact risk, and that firms were often failing to consider the wider risks of identity fraud which could occur from cases of significant data loss and the impact of this on consumers. The *FSA* found that firms lacked a clear understanding of these risks and were therefore failing properly to inform customers, resulting in a lack of transparency.

6.1.5 The contents of this report are reflected in ■ FCG 2 (Financial crime systems and controls) and ■ FCG 5 (Data security).