

Chapter 7

Review of financial crime controls in offshore centres (2008)



7.1 Introduction

7.1.1	<p>Who should read this chapter? This chapter is relevant to:</p> <ul style="list-style-type: none">•all firms subject to the financial crime rules in ■ SYSC 3.2.6R or ■ SYSC 6.1.1R; and•e-money institutions and payment institutions within our supervisory scope who have or are considering establishing operations in offshore centres.
7.1.2	<p>In the second half of 2008 the <i>FSA</i> reviewed how financial services firms in the UK were addressing financial crime risks in functions they had moved to offshore centres. The review followed on from the <i>FSA</i>’s report into data security in financial services (April 2008 – http://www.fsa.gov.uk/pubs/other/data_security.pdf).</p>
7.1.3	<p>The main financial crime risks the <i>FSA</i> reviewed were: customer data being lost or stolen and used to facilitate fraud; money laundering; and fraud. The review found that, while there were good data security controls in place across the industry, continued effort was required to ensure controls did not break down and that they remained ‘valid and risk-based’.</p>
7.1.4	<p>The review emphasised the importance of appropriate vetting and training of all staff, particularly with regard to local staff who had financial crime responsibilities. An examination revealed that training in this area was often lacking and not reflective of the needs of, and work done by, members of staff. The report emphasised that senior management should ensure that staff operating in these roles were given proper financial crime training as well as ensuring they possessed the appropriate technical know-how. The review also highlighted that, due to high staff turnover, firms needed appropriate and thorough vetting controls to supplement inadequate local electronic intelligence and search systems.</p>
7.1.5	<p>The contents of this report are reflected in ■ FCG 2 (Financial crime systems and controls) and ■ FCG 5 (Data security).</p>