

## Chapter 8

# Financial services firms' approach to UK financial sanctions (2009)

## 8.1 Introduction

- 8.1.1** **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.
- 8.1.2** In April 2009 the *FSA* published the findings of our thematic review of firms' approach to UK financial sanctions. The *FSA* received 228 responses to an initial survey from a broad range of firms across the financial services industry, ranging from small firms to major financial groups, both retail and wholesale. Tailored surveys were sent to different types of firms to ensure that the questions were relevant to the nature and scale of the business of each firm. The *FSA* then selected a sub-sample of 25 firms to visit to substantiate the findings from the surveys.
- 8.1.3** The review highlighted areas where there was significant scope across the industry for improvement in firms' systems and controls to comply with the UK financial sanctions regime. The *FSA* found that, while some firms had robust systems in place that were appropriate to their business need, others, including some major firms, lacked integral infrastructure and struggled with inappropriate systems for their business. In small firms in particular, the *FSA* found a widespread lack of awareness of the UK financial sanctions regime.
- 8.1.4** The report examined a number of key areas of concern which included an in-depth look at whether senior management were aware of their responsibilities and, if so, were responding in an appropriate manner. The *FSA* also identified issues over the implementation of policies and procedures, particularly those put in place to ensure that staff were adequately trained, were kept aware of changes in this area, and knew how to respond when sanctions were imposed. The *FSA* also had concerns about firms' screening of clients, both initially and as an ongoing process.
- 8.1.5** The contents of this report are reflected in ■ FCG 2 (Financial crime systems and controls) and ■ FCG 7 (Sanctions and asset freezes).



## **8.2 The FSA's findings**

### **8.2.1**

You can read the findings of the *FSA's* thematic review here: [http://www.fsa.gov.uk/pubs/other/Sanctions\\_final\\_report.pdf](http://www.fsa.gov.uk/pubs/other/Sanctions_final_report.pdf)



## 8.3 Consolidated examples of good and poor practice

### 8.3.1

#### Senior management responsibility

Examples of good practice	Examples of poor practice
<ul style="list-style-type: none"> <li>• Senior management involvement in approving and taking responsibility for policies and procedures.</li> </ul>	<ul style="list-style-type: none"> <li>• No senior management involvement or understanding regarding the firm’s obligations under the UK financial sanctions regime, or its systems and controls to comply with it.</li> </ul>
<ul style="list-style-type: none"> <li>• A level of senior management awareness of the firm’s obligations regarding financial sanctions sufficient to enable them to discharge their functions effectively.</li> </ul>	<ul style="list-style-type: none"> <li>• No, or insufficient, management oversight of the day-to-day operation of systems and controls.</li> </ul>
<ul style="list-style-type: none"> <li>• Appropriate escalation in cases where a potential target match cannot easily be verified.</li> </ul>	<ul style="list-style-type: none"> <li>• Failure to included assessments of the financial sanctions systems and controls as a normal part of internal audit programmes.</li> </ul>
<ul style="list-style-type: none"> <li>• Adequate and appropriate resources allocated by senior management.</li> </ul>	<ul style="list-style-type: none"> <li>• No senior management involvement in any cases where a potential target match cannot easily be verified.</li> </ul>
<ul style="list-style-type: none"> <li>• Appropriate escalation of actual target matches and breaches of UK financial sanctions.</li> </ul>	<ul style="list-style-type: none"> <li>• Senior management never being made aware of a target match or breach of sanctions for an existing customer.</li> <li>• Failure to notify customers affected by data loss in case the details are picked up by the media.</li> </ul>

### 8.3.2

#### Risk assessment

Examples of good practice	Examples of poor practice
<ul style="list-style-type: none"> <li>• Conducting a comprehensive risk assessment, based on</li> </ul>	<ul style="list-style-type: none"> <li>• Not assessing the risks that the firm may face of</li> </ul>

<p>a good understanding of the financial sanctions regime, covering the risks that may be posed by clients, transactions, services, products and jurisdictions.</p> <ul style="list-style-type: none"> <li>• Taking into account associated parties, such as directors and beneficial owners.</li> <li>• A formal documented risk assessment with a clearly documented rationale for the approach.</li> </ul>	<p>breaching financial sanctions.</p> <ul style="list-style-type: none"> <li>• Risk assessments that are based on misconceptions.</li> </ul>
---	--

**8.3.3**

**Policies and procedures**

Examples of good practice	Examples of poor practice
<ul style="list-style-type: none"> <li>• Documented policies and procedures in place, which clearly set out a firm’s approach to complying with its legal and regulatory requirements in this area.</li> <li>• Group-wide policies for UK financial sanctions screening, to ensure that business unit-specific policies and procedures reflect the standard set out in group policy.</li> <li>• Effective procedures to screen against the Consolidated List (See FCG Annex 1 for descriptions of common terms) that are appropriate for the business, covering customers, transactions and services across all products and business lines.</li> <li>• Clear, simple and well understood escalation procedures to enable staff to raise financial sanctions concerns with management.</li> <li>• Regular review and update of policies and procedures.</li> <li>• Regular reviews of the effectiveness of policies, procedures, systems and controls by the firm’s internal audit function or another independent party.</li> <li>• Procedures that include ongoing monitoring/screening of clients.</li> </ul>	<ul style="list-style-type: none"> <li>• No policies or procedures in place for complying with the legal and regulatory requirements of the UK financial sanctions regime.</li> <li>• Internal audits of procedures carried out by persons with responsibility for oversight of financial sanctions procedures, rather than an independent party.</li> </ul>

**8.3.4**

**Staff training and awareness**

Examples of good practice	Examples of poor practice
<ul style="list-style-type: none"> <li>Regularly updated training and awareness programmes that are relevant and appropriate for employees’ particular roles.</li> <li>Testing to ensure that employees have a good understanding of financial sanctions risks and procedures.</li> <li>Ongoing monitoring of employees’ work to ensure they understand the financial sanctions procedures and are adhering to them.</li> <li>Training provided to each business unit covering both the group-wide and business unit-specific policies on financial sanctions.</li> </ul>	<ul style="list-style-type: none"> <li>No training on financial sanctions.</li> <li>Relevant staff unaware of the firm’s policies and procedures to comply with the UK financial sanctions regime.</li> <li>Changes to the financial sanctions policies, procedures, systems and controls are not communicated to relevant staff.</li> </ul>

**8.3.5**

**Screening during client take-on**

Examples of good practice	Examples of poor practice
<ul style="list-style-type: none"> <li>An effective screening system appropriate to the nature, size and risk of the firm’s business.</li> <li>Screening against the Consolidated List at the time of client take-on before providing any services or undertaking any transactions for a customer.</li> <li>Screening directors and beneficial owners of corporate customers.</li> <li>Screening third party payees where adequate information is available.</li> <li>Where the firm’s procedures require dual control (e.g. a ‘four eyes’ check) to be used, having in place an effective process to ensure this happens.</li> </ul>	<ul style="list-style-type: none"> <li>Screening only on notification of a claim on an insurance policy, rather than during client take-on.</li> <li>Relying on other FSA-authorized firms and compliance consultants to screen clients against the Consolidated List without taking reasonable steps to ensure that they are doing so effectively.</li> <li>Assuming that AML customer due diligence checks include screening against the Consolidated List.</li> <li>Failing to screen UK-based clients on the assumption that there are no UK-based persons or entities on the Consolidated List or failure to screen due to any other misconception.</li> <li>Large global institutions with millions of clients using manual screening, increasing the likelihood of human error and leading to matches being missed.</li> </ul>

- The use of ‘fuzzy matching’ where automated screening systems are used.
- Where a commercially available automated screening system is implemented, making sure that there is a full understanding of the capabilities and limits of the system.
- IT systems that cannot flag potential matches clearly and prominently.
- Firms calibrating their screening rules too narrowly or too widely so that they, for example, match only exact names with the Consolidated List or generate large numbers of resource intensive false positives.
- Regarding the implementation of a commercially available sanctions screening system as a panacea, with no further work required by the firm.
- Failing to tailor a commercially available sanctions screening system to the firm’s requirements.

**8.3.6**

Ongoing screening

Examples of good practice	Examples of poor practice
<ul style="list-style-type: none"> <li>• Screening of the entire client base within a reasonable time following updates to the Consolidated List.</li> </ul>	<ul style="list-style-type: none"> <li>• No ongoing screening of customer databases or transactions.</li> </ul>
<ul style="list-style-type: none"> <li>• Ensuring that customer data used for ongoing screening is up to date and correct.</li> </ul>	<ul style="list-style-type: none"> <li>• Failure to screen directors and beneficial owners of corporate customers and/or third party payees where adequate information is available.</li> </ul>
<ul style="list-style-type: none"> <li>• Processes that include screening for indirect as well as direct customers and also third party payees, wherever possible.</li> </ul>	<ul style="list-style-type: none"> <li>• Failure to review the calibration and rules of automated systems, or to set the calibration in accordance with the firm’s risk appetite.</li> </ul>
<ul style="list-style-type: none"> <li>• Processes that include screening changes to corporate customers’ data (e.g. when new directors are appointed or if there are changes to beneficial owners).</li> </ul>	<ul style="list-style-type: none"> <li>• Flags on systems that are dependent on staff looking for them.</li> </ul>
<ul style="list-style-type: none"> <li>• Regular reviews of the calibration and rules of automated systems to ensure they are operating effectively.</li> </ul>	<ul style="list-style-type: none"> <li>• Controls on systems that can be overridden without referral to compliance.</li> </ul>
<ul style="list-style-type: none"> <li>• Screening systems calibrated in accordance with the firm’s risk appetite, rather than the settings sug-</li> </ul>	

- gested by external software providers.
- Systems calibrated to include ‘fuzzy matching’, including name reversal, digit rotation and character manipulation.
- Flags on systems prominently and clearly identified.
- Controls that require referral to relevant compliance staff prior to dealing with flagged individuals or entities.

**8.3.7**

**Treatment of potential target matches**

Examples of good practice	Examples of poor practice
<ul style="list-style-type: none"> <li>• Procedures for investigating whether a potential match is an actual target match or a false positive.</li> </ul>	<ul style="list-style-type: none"> <li>• No procedures in place for investigating potential matches with the Consolidated List.</li> </ul>
<ul style="list-style-type: none"> <li>• Procedures for freezing accounts where an actual target match is identified.</li> </ul>	<ul style="list-style-type: none"> <li>• Discounting actual target matches incorrectly as false positives due to insufficient investigation.</li> </ul>
<ul style="list-style-type: none"> <li>• Procedures for notifying the Treasury’s AFU promptly of any confirmed matches.</li> </ul>	<ul style="list-style-type: none"> <li>• No audit trail of decisions where potential target matches are judged to be false positives.</li> </ul>
<ul style="list-style-type: none"> <li>• Procedures for notifying senior management of target matches and cases where the firm cannot determine whether a potential match is the actual target on the Consolidated List.</li> </ul>	
<ul style="list-style-type: none"> <li>• A clear audit trail of the investigation of potential target matches and the decisions and actions taken, such as the rationale for deciding that a potential target match is a false positive.</li> </ul>	