Chapter 7

Sanctions and asset freezes

7.2 Themes

Governance

7.2.1 G The guidance in ■ FCG 2.2.1G on governance in relation to financial crime also applies to sanctions.

Senior management should be sufficiently aware of the firm's obligations regarding financial sanctions to enable them to discharge their functions effectively.

Self-assessment questions:

- Has your firm **clearly allocated** responsibility for adherence to the sanctions regime? To whom?
- How does the firm **monitor performance**? (For example, statistical or narrative reports on matches or breaches.)

Examples of good practice	Examples of poor practice
• An individual of **sufficient authority** is responsible for overseeing the firm's adherence to the sanctions regime.	• The firm believes payments to sanctioned individuals and entities are **permitted** when the sums are small. Without a licence from the Asset Freezing Unit, this could be a **criminal offence**.
• It is clear **at what stage customers are screened** in different situations (e.g. when customers are passed from agents or other companies in the group).	• No **internal audit** resource is allocated to monitoring sanctions compliance.
• There is **appropriate escalation** of actual target matches and breaches of UK sanctions. Notifications are timely.	• Some business units in a large organisation think they are **exempt**.

The offence will depend on the sanctions provisions breached.

Risk assessment

7.2.2 G The guidance in ■ FCG 2.2.4G on risk assessment in relation to financial crime also applies to sanctions.

A firm should consider which areas of its business are most likely to provide services or resources to individuals or entities on the Consolidated List.

Self-assessment questions:

•Does your firm have a **clear view** on where within the firm breaches are most likely to occur? (This may cover different business lines, sales channels, customer types, geographical locations, etc.)

•How is the risk assessment **kept up to date**, particularly after the firm enters a new jurisdiction or introduces a new product?

Examples of good practice	Examples of poor practice
• A firm with international operations, or that deals in currencies other than sterling, understands the requirements of relevant **local financial sanctions regimes**.	• There is **no process** for updating the risk assessment.
• A small firm is **aware** of the sanctions regime and where it is most vulnerable, even if risk assessment is only informal.	• The firm assumes financial sanctions **only apply to money transfers** and so has not assessed its risks.

Screening customers against sanctions lists

7.2.3 G A firm should have effective, up-to-date screening systems appropriate to the nature, size and risk of its business. Although screening itself is not a legal requirement, screening new customers and payments against the Consolidated List, and screening existing customers when new names are added to the list, helps to ensure that firms will not breach the sanctions regime. (Some firms may knowingly continue to retain customers who are listed under UK sanctions: this is permitted if OFSI has granted a licence.)

Self-assessment questions:

•When are customers screened against **lists**, whether the Consolidated List, internal watchlists maintained by the firm, or lists from commercial providers? (Screening should take place at the time of customer take-on. Good reasons are needed to justify the risk posed by retrospective screening, such as the existence of general licences.)

•If a customer was **referred** to the firm, how does the firm ensure the person is not listed? (Does the firm screen the customer against the list itself, or does it seek assurances from the referring party?)

•How does the firm become **aware of changes** to the Consolidated List? (Are there manual or automated systems? Are customer lists rescreened after each update is issued?)

Examples of good practice	Examples of poor practice
• The firm has considered what **mixture** of manual and automated screening is most appropriate.	• The firm assumes that an intermediary has screened a customer, but **does not check** this.
• There are quality control checks over **manual screening**.	• Where a firm uses automated systems, it does not understand how to **calibrate** them and does not check whether

Examples of good practice	Examples of poor practice
	the number of hits is unexpectedly high or low.
• Where a firm uses automated systems these can make '**fuzzy matches**' (e.g. able to identify similar or variant spellings of names, name reversal, digit rotation, character manipulation, etc.).	• An insurance company **only screens when claims** are made on a policy.
• The firm screens customers' **directors** and known **beneficial owners** on a risk-sensitive basis.	• Screening of customer databases is a **one-off** exercise.
• Where the firm maintains an account for a listed individual, the status of this account is **clearly flagged** to staff.	• Updating from the Consolidated List is **haphazard**. Some business units use out-of-date lists.
• A firm only places faith in **other firms' screening** (such as outsourcers or intermediaries) after taking steps to satisfy themselves this is appropriate.	• The firm has **no means** of monitoring payment instructions.

7

Matches and escalation

7.2.4 G When a customer's name matches a person on the Consolidated List it will often be a 'false positive' (e.g. a customer has the same or similar name but is not the same person). Firms should have procedures for identifying where name matches are real and for freezing assets where this is appropriate.

Self-assessment questions:

•What steps does your firm take to identify whether **a name match is real**? (For example, does the firm look at a range of identifier information such as name, date of birth, address or other customer data?)

•Is there a **clear procedure** if there is a breach? (This might cover, for example, alerting senior management, the Treasury and the *FCA*, and giving consideration to a Suspicious Activity Report.)

Examples of good practice	Examples of poor practice
• Sufficient resources are available to identify '**false positives**'.	• The firm **does not report a breach** of the financial sanctions regime to OFSI: **this could be a criminal offence**.

Examples of good practice	Examples of poor practice
• After a breach, as well as meeting its formal obligation to notify **OFSI**, the firm considers whether it should report the breach to the *FCA*. SUP 15.3 contains general notification requirements. Firms are required to tell us, for example, about significant rule breaches (see SUP 15.3.11R(1)). Firms should therefore consider whether the breach is the result of any matter within the scope of SUP 15.3, for example a significant failure in their financial crime systems and controls.	• An account is **not frozen** when a match with the Consolidated List is identified. If, as a consequence, funds held, owned or controlled by a designated person are dealt with or made available to the designated person, **this could be a criminal offence**. • A **lack of resources** prevents a firm from **adequately analysing** matches. • **No audit trail** of decisions where potential target matches are judged to be false positives.

The offence will depend on the sanctions provisions breached.

Weapons proliferation

7.2.5 G Alongside financial sanctions, the government imposes controls on certain types of trade in order to achieve foreign policy objectives. The export of goods and services for use in nuclear, radiological, chemical or biological weapons programmes is subject to strict controls. Firms' systems and controls should address the proliferation risks they face.

Self-assessment questions:

•Does your firm finance trade with **high risk countries**? If so, is **enhanced due diligence** carried out on counterparties and goods? Where doubt remains, is evidence sought from exporters that the trade is legitimate?

•Does your firm have **customers from high risk countries**, or with a history of dealing with individuals and entities from such places? If so, has the firm reviewed how the sanctions situation could affect such counterparties, and discussed with them how they may be affected by relevant regulations?

•What **other business** takes place with high risk jurisdictions, and what measures are in place to contain the risks of transactions being related to proliferation?

Examples of good practice	Examples of poor practice
• A bank has identified if its customers export goods to high risk jurisdictions, and subjects transactions to **enhanced**	• The firm **assumes** customers selling goods to countries of concern will have checked the exports are legitimate, and

Examples of good practice	Examples of poor practice
scrutiny by identifying, for example, whether goods may be subject to export restrictions, or end-users may be of concern.	**does not ask for evidence** of this from customers.
• Where **doubt exists**, the bank asks the customer to **demonstrate** that appropriate assurances have been gained from relevant government authorities.	• A firm knows that its customers deal with individuals and entities from high risk jurisdictions but **does not communicate with those customers** about relevant regulations in place and how they affect them.
• The firm has considered **how to respond** if the government takes action under the Counter-Terrorism Act 2008 against one of its customers.	• [deleted]

Case study – deficient sanctions systems and controls

7.2.6 G In August 2010, the *FSA* fined Royal Bank of Scotland (RBS) £5.6m for deficiencies in its systems and controls to prevent breaches of UK financial sanctions.

•RBS failed adequately to screen its customers – and the payments they made and received – against the sanctions list, thereby running the risk that it could have facilitated payments to or from sanctioned people and organisations.

•The bank did not, for example, screen cross-border payments made by its customers in sterling or euros.

•It also failed to ensure its 'fuzzy matching' software remained effective, and, in many cases, did not screen the names of directors and beneficial owners of customer companies.

The failings led the *FSA* to conclude that RBS had breached the Money Laundering Regulations 2007, and our penalty was imposed under that legislation – a first for the *FSA*.

For more information see the *FSA's* press release: www.fsa.gov.uk/pages/Library/Communication/PR/2010/130.shtml