# Chapter 7

# Sanctions and asset freezes

## 7.1 Introduction

7.1.1 G **Who should read this chapter?** All firms are required to comply with the UK's financial sanctions regime. The *FCA's* role is to ensure that the firms it supervises have adequate systems and controls to do so. As such, this chapter applies to **all firms** subject to the financial crime rules in ■ SYSC 3.2.6R or ■ SYSC 6.1.1R. It also applies to **e-money institutions and payment institutions** within our supervisory scope.

7.1.2 G Firms' systems and controls should also address, where relevant, the risks they face from weapons proliferators, although these risks will be very low for the majority of *FSA*-supervised firms. ■ FCG 7.2.5G, which looks at weapons proliferation, applies to **banks carrying out trade finance business** and those engaged in other activities, such as **project finance** and **insurance**, for whom the risks are greatest.

7.1.3 G [deleted]

7.1.4 G Financial sanctions are restrictions put in place by the UK government or the multilateral organisations that limit the provision of certain financial services or restrict access to financial markets, funds and economic resources in order to achieve a specific foreign policy or national security objective.

7.1.5 G All individuals and legal entities who are within or undertake activities within the UK's territory must comply with the EU and UK financial sanctions that are in force. All UK nationals and UK legal entities established under UK law, including their branches, must also comply with UK financial sanctions that are in force, irrespective of where their activities take place.

7.1.5A G The Office of Financial Sanctions (OFSI) within the Treasury maintains a Consolidated List of financial sanctions targets designated by the United Nations, the European Union and the United Kingdom, which is available from its website. If firms become aware of a breach, they must notify OFSI in accordance with the relevant provisions. OFSI have published guidance on complying with UK obligations and this is available on their website. See https://www.gov.uk/government/publications/financial-sanctions-faqs.

7.1.6 G Alongside financial sanctions, the government imposes controls on certain types of trade. As part of this, the export of goods and services for use in nuclear, radiological, chemical or biological weapons programmes is subject to strict controls. Proliferators seek to gain access to this technology illegally:

aiding them is an offence under the Anti-Terrorism, Crime and Security Act 2001. Note that the Treasury can also use powers under the Counter Terrorism Act 2008 (see ■ FCG Annex 1) to direct financial firms to, say, cease business with certain customers involved in proliferation activity.

## 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**. |
| • 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 | • 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 des- |

| Examples of good practice | Examples of poor practice |
|---|---|
| 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. | ignated person, **this could be a criminal offence**.<br>• A **lack of resources** prevents a firm from **adequately analysing** matches.<br>• **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 scrutiny** by identifying, for example, whether goods may be subject to export restrictions, or end-users may be of concern. | • The firm **assumes** customers selling goods to countries of concern will have checked the exports are legitimate, and **does not ask for evidence** of this from customers. |

| Examples of good practice | Examples of poor practice |
|---|---|
| • 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

## 7.3 Further guidance

7.3.1 G *FCTR* contains the following additional material on sanctions and assets freezes:

- FCTR 8 summarises the findings of the *FSA's* thematic review Financial services firms' approach to UK financial sanctions and includes guidance on:
  - Senior management responsibility (FCTR 8.3.1G)
  - Risk assessment (FCTR 8.3.2G)
  - Policies and procedures (FCTR 8.3.3G)
  - Staff training and awareness (FCTR 8.3.4G)
  - Screening during client take-on (FCTR 8.3.5G)
  - Ongoing screening (FCTR 8.3.6G)
  - Treatment of potential target matches (FCTR 8.3.7G)
- FCTR 15 summarises the findings of the *FCA's* thematic review Banks' management of financial crime risk in trade finance and includes guidance on:
  - Sanctions Procedures (FCTR 15.3.7G)
  - Dual-Use Goods (FCTR 15.3.8G)

## 7.4 Sources of further information

7.4.1 G To find out more on financial sanctions, see:

- OFSI's website: https://www.gov.uk/government/organisations/office-of-financial-sanctions-implementation
- OFSI provides FAQs on financial sanctions- https://www.gov.uk/government/publications/financial-sanctions-faqs
- Part III of the Joint Money Laundering Steering Group's guidance, which is a chief source of guidance for firms on this topic: www.jmlsg.org.uk

7.4.2 G To find out more on trade sanctions and proliferation, see:

- Part III of the Joint Money Laundering Steering Group's guidance on the prevention of money laundering and terrorist financing, which contains a chapter on proliferation financing that should be firms' chief source of guidance on this topic: www.jmlsg.org.uk
- The website of the UK's Export Control Organisation, which contains much useful information, including lists of equipment requiring a licence to be exported to any destination, because they are either military items or 'dual use' https://www.gov.uk/government/organisations/export-control-organisation
- The NCA's website, which contains guidelines on how to report suspicions related to weapons proliferation:http://www.nationalcrimeagency.gov.uk/publications/suspicious-activity-reports-sars/57-sar-guidance-notes
- The FATF website. In June 2008, FATF launched a 'Proliferation Financing Report' that includes case studies of past proliferation cases, including some involving UK banks. This was followed up with a report in February 2010:https://www.fatf-gafi.org/media/fatf/documents/reports/Typologies%20Report%20on%20Proliferation%20Financing.pdf . http://www.fatf-gafi.org/media/fatf/documents/reports/Status-report-proliferation-financing.pdf.