Chapter 7

Sanctions, asset freezes and proliferation financing

7.1 Introduction

7

7.1.1 G **Who should read this chapter?** All firms are required to comply with UK financial sanctions. 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 and the cryptoasset sector** 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 *FCA*-supervised firms. ■ FCG 7.2.5G, which looks at weapons proliferation, applies to all firms subject to our supervision.

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 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.

Under *Principle* 11 (■ PRIN 2.1.1R), we expect authorised firms to notify us if they (or their group companies, *approved persons*, *senior management functions*, *appointed representatives* and *agents*) are targets **of UK** sanctions **or those of any other country or jurisdiction**.

For firms such as *electronic money institutions*, payment services firms, *cryptoasset businesses* and Annex I financial institutions, this is regarded as a material change of circumstance and we expect to be informed if you or any connected entities are **targets of UK** sanctions **or those of any other country or jurisdiction**.

7.1.5A G The Office of Financial Sanctions (OFSI) within the Treasury helps to ensure that financial sanctions are properly understood, implemented and enforced in the United Kingdom. HM Government publishes the UK Sanctions List, which provides details of those designated under regulations made under the Sanctions and Anti-Money Laundering Act. The list also details which

sanctions measures apply to these persons or ships. OFSI maintains a Consolidated List of financial sanctions targets designated by the United Nations 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.

Firms should also consider whether they should report sanctions breaches 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 a sanctions 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.

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

7.2.-1 G The guidance set out in ■ FCG 2.2 (Themes) and ■ FCG 2.3 (Further guidance) also applies to sanctions.

Governance

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

We expect senior management to take clear responsibility for managing sanctions risks, which should be treated in the same manner as other risks faced by the business. There should be evidence that senior management are actively engaged in the firm's approach to addressing the risks of non-compliance with UK financial sanctions. Where they identify gaps, they should remediate them.

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.)
- How are **senior management** kept **up to date** with sanctions compliance issues?
- Does the firm's organisational structure with respect to sanctions compliance across **different jurisdictions** promote a **coordinated approach and accountability**?
- Does the firm have **evidence** that sanctions issues are **escalated** where warranted?
- Where sanctions controls processes rely on resource external to the firm, is there **appropriate oversight** and **understanding** of that resource?

Examples of good practice	Examples of poor practice
• An individual of **sufficient authority** is responsible for overseeing the firm's adherence to UK sanctions.	• The firm believes payments to sanctioned individuals and entities are **permitted** when the sums are small. Without a licence from the OFSI, this could be a **criminal offence**.

Examples of good practice	Examples of poor practice
	• Multinational firms **lack** the **communication** between global and regional sanctions teams necessary to **manage** compliance with UK sanctions laws, regulations and guidance.
• 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.

Management information (MI)

7.2.1A G The guidance in ■ FCG 2.2.2G on MI in relation to financial crime also applies to sanctions.

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

Self-assessment questions:

- How does your firm **monitor performance**? (For example, statistical or narrative reports on matches or breaches.)
- Does **regular and ad hoc MI** provide senior management with a clear understanding of the firm's sanctions compliance risk?
- Is the MI produced relevant to UK sanctions?

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 and proliferation financing (PF) (see ■ FCG 7.2.5G for PF).

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;
- are owned and controlled by individuals or entities on the Consolidated List;
- engage in services or transactions prohibited under UK financial sanctions; or
- rely on prohibited suppliers, intermediaries or counterparties.

Self-assessment questions:

•Does your firm have a **clear view** on where within the firm **potential sanctions 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 or where **it has identified new sanctions risk events**?

•Has senior management set a clear **risk appetite** in relation to its sanctions risks, including in its exposure to sanctioned persons, activities and **jurisdictions**?

•Does your firm have established **risk metrics** to help detect and manage its sanctions compliance exposure on an ongoing basis?

•Are there established **procedures** to identify and escalate new sanctions risk events, such as new sanctions regimes, sanctioned activities and evasion typologies?

•Is your firm utilising available guidance and resources on **new and emerging** sanctions evasion typologies?

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.
• The firm conducts **contingency planning**, taking a proactive approach to identifying sanctions exposure and is conducting exposure assessments and scenario planning. The firm updates business-wide and customer risk assessments to **account for changes** in the nature and type of sanctions measures.	
• The firm **performs lessons learned** exercises following material sanctions developments to improve its readiness to respond to future events.	
• The firm engages with **public-private partnerships and private-private partnerships** to gather insights on the latest typologies and additional controls that might be relevant	

Examples of good practice	Examples of poor practice
and share its own best practice examples.	

Customer due diligence checks

7.2.2A G

As well as being relevant to other financial crime controls, effective customer due diligence (CDD) and know your customer (KYC) assessments are a cornerstone of effective compliance with sanctions requirements.

Examples of good practice	Examples of poor practice
• Sanctions risk is **proactively** included into the firm's CDD process.	• The firm has **low-quality** CDD and KYC assessments and **review backlogs**, raising the risk of not identifying sanctioned individuals and entities.
• The firm's CDD identifies **all parties** relevant for its screening processes.	• The firm's CDD processes are **unable to identify** connected parties and corporate structures that may be subject to sanctions.
• The firm's customer onboarding and due diligence processes **are designed to identify** customers who make use of **corporate vehicles** to obscure ownership or source of funds.	• The firm's CDD **does not articulate** full ownership structures of entities and the firm is unable to show that it is screening all relevant parties.
• The firm **has processes designed** to **identify** activity that is **not in line with the customer profile** or is otherwise **suspicious**.	

7.2.2B G

Further guidance on good and bad practice relating to CDD checks can be found in ■ FCG 3.2.4G.

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, counterparties to transactions 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 UK sanctions.

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?)

•Does your firm have a **clear policy** on which customers, counterparties and payments are subject to screening, and what related data is subject to screening?

•Does your firm have **service level agreements** that cover how quickly it updates its sanctions screening lists following updates to the Consolidated List and that are appropriate to the sanctions risks of its business?

•Does your firm **evaluate** its **screening capabilities** so that its screening system is adequately calibrated for its needs and to monitor UK sanctions? Do you regularly **test/measure** the effectiveness of the system?

•Is the team responsible for sanctions compliance properly **resourced and skilled** to effectively perform sanctions screening **and alert management**?

•If using an outsourced service, does your firm have appropriate **control and oversight** of its sanctions screening controls?

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 the number of hits is unexpectedly high or low.
• The firm **understands its automated** screening tool and how it is calibrated, and is able to demonstrate that it is appropriate to the firm's risk exposure.	• Calibration is **not adequately tailored** and the system is either too sensitive or not sensitive enough. This may result in name variations not being detected, for example.
• The firm is able to show the controls in place to **measure the effectiveness** of **its auto**	• There is **limited or no understanding** by the firm about how a third-party tool is calib-

Examples of good practice	Examples of poor practice
mated system, thresholds and parameters – for instance, with sample testing and tuning.	rated and when lists are updated.
• 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.). The firm continually seeks ways to enhance the system to help identify **potential** sanctions **breaches**.	• 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 or entity, 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 relies on **other firms' screening** (such as outsourcers or intermediaries) after taking steps to satisfy itself this is appropriate.	• The firm is **overly reliant** on a third-party provider screening solution, with no oversight. The firm has **no means** of monitoring payment instructions.
• The screening tool is **calibrated and tailored** to the firm's **risk** and **is** appropriate for **screening UK sanctions**. Customers and their transactions are screened against relevant updated sanctions lists and effective re-screening is in place to identify activity that may indicate sanctions breaches.	
• Where **blockchain analytics** solutions are deployed, the firm ensures that compliance teams **understand** how these capabilities can be best used to identify transactions linked to higher risk wallet addresses, **including those included on the Consolidated List**.	
• The firm's sanctions teams are adequately **resourced** to avoid backlogs in sanctions screening and are able to react to those at pace.	• The firm **lacks proper resources** and **expertise** to ensure effective screening **and investigation of alerts**. It has significant backlogs and faces the risk of non-compliance with its obligations.

Examples of good practice	Examples of poor practice
	• Increased volumes and pressure on sanctions teams **following changes in the sanctions landscape prevent** firms from taking **appropriate and timely action** for true positive alerts and increase the risk of errors. There is a lack of clarity around prioritisation of alerts, internal service level agreements and governance.

Evasion detection and investigation

7.2.3A G

A firm should have effective, up-to-date screening systems appropriate to the nature, size and risk of its business. However, simple screening of names against the Consolidated List may not always identify potential sanctions evasion involving third parties and alternative detection techniques may be needed. **Potential red flags for sanctions evasion are set out in alerts issued by the National Economic Crime Centre (NECC)**.

Self-assessment questions:

•Does your firm understand potential sanctions **evasion typologies** relevant to its business and has it considered how to detect them?

•Has your firm considered whether **additional procedures are needed** to identify potential sanctions evasion?

Examples of good practice	Examples of poor practice
• The firm is using techniques, such as data analytics, to identify customers who may be close associates or dependents or have transactional links with designated persons, and so may **represent a higher risk** of sanctions non-compliance.	

Asset freezing and licenses

7.2.3B G

When a financial sanction is an asset freeze, the funds and economic resources belonging to or owned, held or controlled by a designated person are generally to be frozen immediately by the person in possession or control of them, unless there is an exception in the legislation they can rely on, or they have a licence from OFSI.

Self-assessment questions:

•Does your firm have **clear policies and procedures** as to when funds and economic resources are frozen or released?

•Have you assessed how any frozen funds and economic resources in your firm's possession or control are **maintained in compliance** with UK sanctions?

•Does your firm have clear policies and procedures to **assess, utilise and monitor** the use of OFSI licences and statutory exceptions?

Reporting and assessing potential sanctions breaches

7.2.3C G Relevant firms are required to report to OFSI where they know or have reasonable cause to suspect a breach of financial sanctions, and notify OFSI if:

•a person they are dealing with, directly or indirectly, is a designated person;

•they hold any frozen assets; or

•they discover or suspect any breach while conducting their business.

In line with *Principle* 11, ■ SUP 15.3.8G(2) and ■ FCG 7, firms must consider whether they need to notify us – for example, whether potential breaches of sanctions resulted from a significant failure in their systems and controls.

Self-assessment questions:

•Is there a clear procedure that sets out what to do if a potential **sanctions breach** is identified? (This might cover, for example, alerting senior management, OFSI and the *FCA*, and giving consideration to whether to submit a Suspicious Activity Report).

•Does your firm consider the **root causes** of any potential sanctions breaches and consider the implications for its policies and procedures?

Examples of good practice	Examples of poor practice
• The firm undertakes **a root cause analysis** of potential sanctions breaches and uses them to update its sanctions controls.	• The firm **does not report a breach** of financial sanctions to OFSI **when required to do so**. This could be a criminal offence.
• After a breach, as well as meeting its formal obligation **to notify OFSI**, the firm **reports the breach to the FCA**. SUP 15.3 contains general notification requirements. Firms are required to tell us about significant *rule* breaches (see SUP 15.3.11R(1)), such as a significant failure in their financial	

Examples of good practice	Examples of poor practice
crime systems and controls. • **Significant deficiencies in the firm's systems and controls resulting in potential sanctions breaches are reported** to the *FCA*.	

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 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.

Examples of good practice	Examples of poor practice
	• **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 and policies and procedures should address and mitigate the proliferation risks they face. Firms are also required to carry out proliferation financing risk assessments under regulation 18A of the *Money Laundering Regulations*, either as part of the existing practice-wide risk assessment or as a standalone document.

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.
• 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	• [deleted]

Examples of good practice	Examples of poor practice
takes action under the Counter-Terrorism Act 2008 against one of its customers.	

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 *FCA's* thematic review of 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: www.jmlsg.org.uk
- OFSI UK Financial Sanctions Guidance: www.gov.uk/government/publications/financial-sanctions-general-guidance/uk-financial-sanctions-general-guidance
- Alerts published by the NECC: www.nationalcrimeagency.gov.uk/who-we-are/publications/
- *FCA* sanctions webpages – these pages include our latest updates and details on how to report sanctions breaches to us:

  www.fca.org.uk/russian-invasion-ukraine

  www.fca.org.uk/firms/financial-crime/financial-sanctions

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: www.nationalcrimeagency.gov.uk/who-we-are/publications/171-sar-guidance-notes/file
- The FATF guidance on proliferation financing:

www.fatf-gafi.org/content/dam/fatf-gafi/reports/Typologies%20Report%20on%20Proliferation%20Financing.pdf

www.fatf-gafi.org/en/publications/Financingofproliferation/Proliferation-financing-risk-assessment-mitigation.html

- HM Government's website, which includes the National Risk Assessment of Proliferation Financing: www.ncsc.gov.uk/collection/board-toolkit/introduction-to-cyber-security-for-board-members

- The Office of Trade Sanctions Implementation (OTSI) helps to ensure that trade sanctions are properly understood, implemented and enforced. OTSI has published guidance regarding trade sanctions, and this is available on its website: www.gov.uk/otsi