4: Compliance with the UK financial sanctions regime

The international and UK legislative frameworks for financial sanctions do not prescribe the processes which firms have to adopt to achieve compliance with their legal obligations. This guidance is intended to provide an indication of the types of controls and processes that firms might adopt in order to enable them to comply with sanctions obligations in an effective and proportionate manner. It is not intended to prescribe the manner in which firms must comply with the regime, as much will depend on the nature of the customer base and the business profile of each individual firm. The guidance is intended to assist firms in designing their own processes.

Although it is not formal guidance that has been given Ministerial approval, this guidance has been discussed with HM Treasury and reflects their input.

Introduction

General

4.1 Sanctions can take the form of any of a range of restrictive/coercive measures. They can include arms embargoes, travel bans, asset freezes, reduced diplomatic links, reductions/cessation of any military relationship, flight bans, suspension from international organisations, withdrawal of aid, trade embargoes, restriction on cultural /sporting links and other.

4.2 This guidance focuses on financial sanctions and asset freezes, although firms must also be aware of the nature and requirements of other sanctions, especially trade embargoes.

4.3 The sanctions regime requires absolute compliance and any person in breach of an obligation under a relevant Statutory Instrument will be guilty of an offence, unless a defence is successfully made out. The nature of the legislation means that firms risk breaching a sanctions obligation as soon as an individual or entity is listed in an EU Regulation, or falls within the remit of a UK Statutory Instrument, the timing of which is outside their control (in contrast to AML approaches, which generally allow firms to set their own timetables on checking and updating customer due diligence details). HMT's intention is ultimately that there is a robust and proportionate response to complying with the sanctions requirements. The penalties for committing an offence are covered in each individual Statutory Instrument. The Terrorist Asset-Freezing etc Act 2010 provides a primary legislative basis for the UK's domestic asset freezing regime .

4.4 Notwithstanding the absolute nature of the regime, firms are likely to focus on implementing appropriate systems and controls to identify persons who are subject to financial sanctions, given their assessment of the likelihood of dealing with such persons and associated risk of breaching their obligations. This may involve less immediate or frequent screening and/or being more selective with regard to those who are screened. Firms should note, however, that any provision of funds or financial services etc to, or failure to freeze the assets of, a sanctioned person will expose the firm to the risk of prosecution.

4.5 The sanctions regime is absolute and this provides a challenge for compliance. Some firms, for example large firms with millions of customers or which process many millions of transactions every day, will use automated screening systems. Other firms with smaller numbers of customers and transactions may achieve compliance through other processes. Firms must use sanctions checking processes that are proportionate to the nature and size of the firm's business and that in their view are likely to identify all true matches.

Code for Crown Prosecutors

4.6 If an individual or a firm breaches a financial sanctions prohibition, it will have committed a criminal offence unless a defence is successfully made out. However, in line with the principles set out in the Code for Crown Prosecutors (see Annex 4-IV), prosecution of a firm or individual would only be likely where the prosecuting authorities consider this to be in the public interest, and where they believe that there is enough evidence to provide a realistic prospect of conviction.

What is the financial sanctions regime?

The UK regime

4.7 There is no single Act of Parliament that sets out the UK financial sanctions regime. The UK regime reflects the requirements of various UN Security Council resolutions, and is implemented by way of EU Regulations and UK Statutory Instruments. There are also EU investment ban and trade sanctions regimes that apply in the UK. Annex 4-I summarises these.

What is a financial sanction?

4.8 Financial sanctions are set out separately in statutory instruments and/or EU Regulations relating to the specific regime. It is generally a criminal offence under the UK implementing legislation directly or indirectly to make funds or economic resources available to or for the benefit of targets on the list unless a licence is obtained from HM Treasury. It is also generally a criminal offence to deal with the funds or economic resources of such targets ("sanctions targets") unless licensed. The terrorism financial sanctions regime also prohibits the provision of financial services to sanctions targets. The prohibitions apply whether dealing directly with targets, or dealing with targets through intermediaries, such as lawyers or accountants. In the case of UK terrorist asset freezing legislation the making available of funds, economic resources and financial services to a person other than the target is only prohibited where to do so would bestow a significant financial benefit on a sanctions target.

4.9 In respect of each prohibition, it is a defence for the provider of the funds, economic resources, or where applicable financial services, not to have known or have had reasonable cause to suspect that the prohibition was being breached.

Penalties

4.10 The penalties for a breach of UK financial sanctions (including breach of EU Regulations containing sanctions, which are applicable in the UK) are set out in the relevant statutory instrument. Any person guilty of an offence is liable on conviction to imprisonment and/or a

fine.

HM Treasury website

4.11 HM Treasury's financial sanctions website includes the sanctions legislation applicable in the UK, HM Treasury's sanctions notifications, Guidance notes and related materials. See http://www.hm-treasury.gov.uk/fin_sanctions_index .htm.

The Consolidated List

4.12 The obligations under the UK financial sanctions regime apply to all firms in the financial sector and not just to banks. In order to assist compliance with the UK regime, the Treasury maintains a 'consolidated list' of individuals and entities that are based in the UK or elsewhere that are subject to financial sanctions. The Consolidated List is available at www.hm-treasury.gov.k/d/sanctionsconlist.pdf.

UK Investment Ban List

4.13 A list of investment ban targets designated by the European Union under legislation relating to current financial sanctions regimes is available at www.hm-treasury.gov.uk/d/investmentban.pdf

4.14 Investment ban targets are not included in the Consolidated List of financial sanctions targets. UK financial firms are prohibited from making new investments in the entities named on the list of investment ban targets. They are not prohibited from making other payments to them or receiving payments from them. This guidance may assist financial institutions in designing processes to prevent new investment in those parties.

Responsibilities

4.15 Responsibilities for the UK sanctions regime lies with three Government departments:

(i) HM Treasury
(ii) The Foreign and Commonwealth Office ("FCO"), and
(iii) The UK Department for Business Innovation and Skills ("BIS").

The Financial Services Authority also has a role in relation to firms' systems and controls. Under its financial crime objective, it requires firms, under Principle 3, to have in place appropriate policies and procedures to counter the risk that they might be used to further financial crime. These include adequate systems and controls to comply with the asset freezing regime. Annex 4-II provides a summary of the responsibilities of the UK authorities.

Overseas jurisdictions

4.16 Where a firm is active in jurisdictions outside the UK, it may be required to comply with the requirements of the sanctions regimes in other jurisdictions. Some jurisdictions' requirements may also apply without a firm having an actual presence in that jurisdiction.

4.17 Firms will need to understand which sanctions regimes impact on which parts of their business and ensure they correctly comply with applicable sanctions while not incorrectly

applying regimes of other jurisdictions to UK business. Annex 4-IV contains links to some useful websites.

Approach, Procedures and Training

Approach – what does an asset freeze do?

4.18 An asset freeze prohibits dealings with the funds or economic resources of a sanctions target. It also prohibits making funds or economic resources (and in relation to those designated under the terrorism regime, financial services) available, directly or indirectly, to or (in the case of those designated under the terrorism regime) for the benefit of sanctions targets. Firms should therefore implement appropriate means of control to prevent breaches of prohibitions. It is a criminal offence for a firm to breach a sanctions prohibition.

4.19 In order to reduce the likelihood of breaching obligations under financial sanctions regimes, firms are likely to focus their resources on areas of their business that carry a greater likelihood of involvement with sanctions targets and where meaningful information on their clients, counterparties and transactions is held. Within this approach, firms are likely to focus their prevention and detection procedures on direct customer relationships, and on transactions, having appropriate regard to other parties involved. However, firms cannot ignore "low risk" areas and must ensure that systems and controls also pay attention to areas where dealings with a sanctions target are unlikely, but possible.

Policy and senior management responsibilities

4.20 Firms should have a sanctions policy that is informed by a thorough understanding of legal requirements applied to an assessment of the risks in their firm. Senior management and/or the Board of a firm should understand the firm's obligations and take responsibility for the firm's sanctions compliance policies and procedures.

Approach tailored to business model

4.21 Firms should take an approach which is appropriate for their business model, when assessing where and how their business is most likely to encounter sanctioned parties, and to focus resources and tailor systems and controls accordingly.

4.22 Firms, particularly those with many different client types, product types and/or geographical markets, should consider carrying out an assessment in order to be able to understand which parts of their business may carry a greater likelihood of breaching the requirements of economic or terrorist-related sanctions. Any assessment may usefully include a high level assessment of the firm's view of its business profile in specific business areas, and information on periodic CDD and other checks relating to those areas.

4.23 An assessment should start with identification and assessment of the issues that have to be managed. A firm should develop its approach in the context of how it might most likely be involved in breaching economic and country-related sanctions. A firm may take into account a range of factors when conducting its assessment, including:

- Its customer, product and activity profiles
- Its distribution channels
- The complexity and volume of its transactions

- Its processes and systems
- Its operating environment
- The screening processes of other parties
- The geographic risk of where it does business
- The sanctions regulations of relevant countries.

Documenting the assessment

4.24 Firms should document the assessment and approach adopted on the basis of that assessment. Firms should also identify where a decision is taken to adopt a different approach where this may go beyond a particular requirement.

Firms' activities outside the UK

4.25 UK sanctions legislation typically applies to UK persons and persons in the UK, including bodies incorporated or constituted under UK law. Where firms operate in a number of countries or territories, a consistent group wide 'umbrella' policy should be established, which can assist local business units in ensuring that their local procedures meet minimum group standards. Firms will also need to take account of any particular local, legal requirements. Foreign subsidiaries of UK firms that have a separate legal personality outside the UK (as distinct from branches) would not be covered by UK sanctions law, but by the law of the jurisdiction in which they are based.

Procedures

4.26 Firms should ensure that appropriate policies and procedures are in place across the organisation. A firm's procedures should be appropriate to its business, and readily accessible and well understood by all relevant staff. Senior management must understand and stress the importance of understanding and complying with the firm's policies and procedures.

4.27 Firms should ensure that their procedures remain up to date and fit for purpose in a changing environment. Firms may use internal review, other appropriate functions or external review to achieve this.

4.28 Firms should ensure that they communicate in a timely manner to relevant staff changes to the sanctions requirements, including any internal changes to systems, procedures and controls.

4.29 Firms should adequately monitor their systems processes and controls to support full compliance with sanctions requirements.

Staff Training

4.30 A firm should have staff training programmes commensurate with its business and risk profile. Firms should consider implementing arrangements for:

- providing material containing the firm's financial sanctions policies and procedures which is readily available and simple to understand;
- providing training that is appropriately tailored for different groups of staff to reflect the

likelihood of different degrees of staff involvement with sanctions issues, including what to do in the event of a reportable match;
- providing refresher training, delivered at appropriate intervals.

Circumvention

4.31 Firms' policies and procedures should include provisions to prohibit and detect attempts to circumvent sanctions, by, for example:

- omitting, deleting or altering information in payment messages for the purpose of avoiding detection of that information by other firms in the payment process, or
- structuring transactions with the purpose of concealing the involvement of a sanctioned party.

Employment contracts should make any such attempt a serious disciplinary offence.

Screening of customers and transactions

4.32 Firms should have processes to manage the risk of conducting business with or on behalf of individuals and entities on the Consolidated List (which includes all the names of sanctioned persons and entities under UN and EU sanctions regimes which have effect in the UK). Firms should consider screening their customers on a periodic basis, and certain transaction data. The Consolidated List is available at www.hm-treasury.gov.uk/d/sanctionsconlist.pdf

Taking a tailored approach

4.33 As already noted, it is for individual firms to assess how best to comply with the financial sanctions legislation within the context of their business activities and profile. The prohibitions in the legislation extend beyond payments made directly to sanctions targets, i.e., payments which are made indirectly to, or which are made to others for the benefit of, sanctions targets are within the scope of the legislation.

4.34 An "indirect payment" is one that is made to someone acting on behalf of the sanctions target. In contrast, the prohibition on making payments to others for the benefit of a sanctions target is intended to prevent payments being made to third parties to satisfy an obligation of that person.

4.35 As explained in paragraphs 4.18ff, firms should adopt an approach informed by the profile of their business model and client base. Firms are likely to focus their screening processes on areas of their business that carry a greater likelihood of involvement with sanctions targets, or their agents, although as outlined earlier, low risk areas cannot be ignored.

Record of screening policy

4.36 Firms should keep a written record of their screening policy and be able to justify the timescales and frequency of screening, resolution of screening matches and regulatory reporting if required.

Review of processes

4.37 Firms should review, and update their processes periodically, so that they remain appropriate

for their needs and ensure that any internal guidance is updated to reflect major changes to the sanctions regime, such as the addition of a new jurisdiction or regime.

Elements of screening process

4.38 The scope and complexity of the screening process will be influenced by the firm's business activities, and according to the profile of the firm. An effective screening process should include the following elements:

- it should flag up potential name matches against the Consolidated List and names against which measures have been issued under the Counter-Terrorism Act
- potential matches should be reviewed by appropriately trained staff
- where matches are confirmed as true, appropriate action should be taken to freeze the account
- true matches should be reported as soon as is practicable to the Asset Freezing Unit at HM Treasury (see paragraphs 4.62ff for the reporting of matches) and
- it should maintain an audit trail of actions around potential and true matches.

Screening software

4.39 Many firms use automated customer screening software provided by a commercial provider; other firms rely on manual screening. Firms may consider whether and what type of screening software to use in line with the nature, size and risk profile of their business. A key element of a screening system is that it will flag potential matches clearly and prominently. Firms should document the reasons for choosing whichever screening method they decide to use.

4.40 Where commercially available automated screening software is implemented, firms should understand its capabilities and limits, and make sure it is tailored to their business requirements, data requirements and risk profile. Firms should also monitor the ongoing effectiveness of automated systems. Where automated screening software is used, firms should be satisfied that they have adequate contingency arrangements should the software fail and should periodically check the software is working as they expect it to.

Legacy systems

4.41 Firms should be alert to any operational issues which may arise from having the risk of customer or transaction data in legacy systems.

'Fuzzy matching'

4.42 It is important to consider "fuzzy matching", as names might be missed if only exact matches are screened. "Fuzzy matching" describes any process that identifies non-exact matches. Fuzzy matching software solutions identify possible matches where data - whether in official lists or in firms' internal records - is misspelled, incomplete, or missing. They are often tolerant of multinational and linguistic differences in spelling, formats for dates of birth, and similar data. A sophisticated system will have a variety of settings, enabling greater or less fuzziness in the matching process.

4.43 Where a firm uses a screening system which has a fuzzy matching capability, it should

ensure that the fuzzy matching process is calibrated as appropriate in line with the risk profile of their business.

4.44 Application of a fuzzy matching process to a screening system will result in the generation of an increased number of apparent matches which have to be checked. The generation and resolution of an undue number of false positives may have a negative impact on the efficacy of the resolution process. Firms should therefore consider the level of appropriate human intervention to assess which results may be false positives.

Use of false personal information

4.45 Sanctioned parties are known to use false personal information to try and evade detection of their illicit activities. Typical approaches are to use name variations, e.g., name reversal and removing numbers from the names of entities, etc. For this reason, many firms use screening tools which screen using several protocols – e.g., name reversal, number removal, number replaced by word, etc.

Outsourcing and reliance

4.46 A firm may outsource screening and/or other financial sanctions compliance processes to a contractor, but will remain fully responsible for discharging all of its regulatory obligations. Firms may therefore consider putting in place an appropriate Service Level Agreement with contractors and should satisfy themselves that the outsourced party is providing an effective service.

4.47 There is no "reliance" provision in the UK financial sanctions regime. When screening customers and related parties that are new to the firm but who are or were already clients of another FSA-authorised firm, firms might choose to consider this in their assessment when determining their screening policy. However, it should not be assumed that such clients have already been screened.

Timing of screening

4.48 All customers should be screened during the establishment of a business relationship or as soon as possible after the business relationship has commenced. Firms should be aware of the risks associated with screening customers after a business relationship has been established and/or services have been provided i.e., that they may transact with a sanctioned party in breach of sanctions prohibitions. Firms must be aware of the absolute restrictions embedded in the financial sanctions regime. Where there is any delay in screening, firms face a risk of breaching the legislation.

4.49 For low-risk business a firm might choose post-event screening, provided the nature of the business allows the firm to prevent movement or withdrawal of the asset(s) concerned until the sanction check has been completed.

4.50 In accordance with a firm's business profile, consideration should be given to how often customer re-screening should be carried out. Some firms carry out regular periodic systems-based screening of their entire customer data. Others develop a programme to re-screen for changes to their customer list and changes to the Consolidated List. Firms should ensure that they have adequate arrangements to screen when changes are made to the Consolidated

List.

Screening of associated parties

4.51 The sanctions prohibitions also apply to both indirect payments to and payments for the benefit of sanctions targets. Where practicable, screening should cover any other related parties, for example beneficial owners (including trustees, or company directors), that are identified by the firm in question as requiring verification under its risk-based approach to customer due diligence. A firm's judgement in these matters will need to be consistent with its approach for AML purposes, and whether or not full identity details are collected.

4.52 Firms may choose not to undertake financial sanctions checks in respect of particular related parties associated with an investment if its assessment considers such checks would be disproportionate in particular cases. Firms should be aware, however, that this will increase the risk of sanctions legislation being breached. Firms may be liable to prosecution in respect of any such breaches.

Dormant accounts

4.53 Firms may wish to consider whether dormant accounts should be screened, and if so how and when they should be screened. This decision is likely to reflect the firm's risk policy, and the availability or otherwise of dormant account data on a system that is able to be screened.

Transaction screening

4.54 Firms should monitor higher-risk payment instructions to assist in preventing a breach of the prohibitions. Transactions screening involves screening of payment information to identify potential sanction targets.

4.55 Transaction screening should take place on a real-time payment basis, i.e., the screening or filtering of relevant payment instructions should be carried out before the transaction is executed.

4.56 Firms will approach transaction screening in line with their assessment of their business risks. Firms are likely to focus on screening international transactions where there is adequate information on third parties, and parties to trade finance deals plus walk-in customers wishing to send payments both within and outside the UK. Firms that operate client money accounts or provide safe custody services are likely to focus on third party payments and asset transfers.

4.57 Banks will wish to consider screening both data in the payment and relevant advice messages (e.g., MT103, MT910, MT202 etc) and for intermediary banks data in the cover payments e.g., MT202COV.

4.58 Factors that firms may consider when determining which transactions should be screened include:

- whether automated screening is possible
- industry best practice
- international / domestic connections

- adequate information to ascertain whether it is a potential match
- materiality of transaction
- the nature of the client's business
- analysis of historical sanction matches

4.59 When funds are received electronically by a financial firm as payee (i.e., not a Payment Service Provider in the transaction – see Part I, paragraph 5.2.11), the name of the payer will typically not be passed on by the PSP to the payee. The payee firm is not expected to screen the payer nor to screen the incoming payment, unless there is reason to believe the payer is not their customer.

4.60 When funds are received electronically by a Payee Payment Services Provider from within the EU, the payer's name and address may not be included in the transfer (as it is not required in the relevant legislation – see section 1: *Transparency in electronic payments (wire transfers)*, paragraph 1.14). The PSP may need to consider whether to request additional information in order to meet its sanctions obligations.

Audit trail and record keeping

4.61 Whether firms screen using automated systems or manually, an audit trail should be maintained for a period of no less than five years. This should record all relevant information to a likely match, how it was resolved and the rationale applied. Firms should ensure that their processes are kept under review, and remain up to date, and appropriate for the needs of the institution.

Reporting matches and breaches of the regime

Assessing possible matches

4.62 Firms may often find it difficult to determine if there are true matches i.e., they involve a sanctioned party. Potential matches should be investigated and reviewed as appropriate to confirm if they are true matches. The majority of matches are likely to be "false positives" and after this is confirmed there will be no need for further review. Sophisticated screening software permits adjustment of screening rules, so as to prevent repetition of specific false matches.

4.63 True matches are where a firm has no doubt that the account held is that of a target of the financial sanctions regime. It is also possible to have a potential match where a name of a customer may appear to match the name of a target included on HM Treasury's Consolidated List. Firms should seek to obtain sufficient information to enable them to confirm or eliminate a partial match. This process should be documented in writing.

What is a false positive?

4.64 A "false positive" is the identification of an apparent match to a record on the Consolidated List (or a party against which measures have been issued under the Counter-Terrorism Act) which is assessed on investigation not to relate to a sanctions target or entity.

4.65 Time constraints are also particularly relevant in the context of payments. Firms may make further enquiry either from the counter-party bank or from their client or both, so as to assist

in determining whether the match is a true match. Firms should seek sufficient information to enable them to confirm or eliminate an potential match. This process should be documented in writing. For cases that are assessed to be not a true match, firms should ensure that there is a clear rationale for deciding that an apparent match is a false positive and that this rationale can be demonstrated.

4.66 Every potential match of a customer account should be checked, and if appropriate investigated. This process should be documented in writing. Firms are advised to keep an appropriate audit trail about every likely match. This is likely to include a record of who made the decision and on what grounds.

Reporting to HM Treasury

4.67 Where firms believe that they hold funds or assets for a sanctioned party, this must always be reported to the Asset Freezing Unit at HM Treasury as soon as practicable – see Annex 4-II. Firms must ensure that they have clear internal and external reporting processes for reporting matches to HM Treasury as soon as practicable and that individuals within the firm dealing with matters in relation to which a report has been made to HM Treasury understand their obligations.

What information to report?

4.68 Firms are generally required to report the following information:

- the information or other matter on which the knowledge or belief is based;
- any information held by the financial institution about the sanctions target by which the person can be identified; and
- the nature and amount or quantity of any funds or economic resources held by the financial institution for the sanctions target.

Legislative reporting requirements

4.69 Firms should comply with the specific requirements of the applicable legislation, which may be contained in a UK Statutory Instrument or in an EU Regulation (available from the HM Treasury sanctions website) as regards their obligations in dealing with sanctioned parties. As legislation relating to different sanctioned parties may vary, the detail of the relevant legislation covering the asset freeze should be examined. Firms may also seek advice from HM Treasury's Asset Freezing Unit on the action required, including where serious practical difficulties arise with regard to compliance.

4.70 In the case of sanctions contained in UK Statutory Instruments, HM Treasury may (depending on the applicable Statutory Instrument) in addition ask any UK person (as defined in the relevant Statutory Instrument) to provide information that they may reasonably require for the purpose of monitoring compliance and detecting evasion of the sanctions regime [see for example the Terrorism (United Nations Measures) Order 2009 Schedule Part I (4)].

Contacting customer's branch

4.71 Where a customer's account has been frozen, firms may need to contact the customer's local branch or appropriate business area informing them of the asset freeze.

Notifying customer of asset freeze - does "tipping off" apply?

4.72 Firms will usually wish to consider notifying the customer or parties to a relevant transaction what action has been taken and the reason for that action. Informing the customer or third parties of a party's sanctioned status is not prohibited (unless the person's designation has been made known to only a restricted number of firms on HM Treasury's restricted access website and HM Treasury has specified that the designation is confidential information and not to be disclosed further). It is not of itself a 'tipping off' offence under the Proceeds of Crime Act 2002 ("POCA"), as the fact that a party is sanctioned is public information (unless it is specified to be confidential in the circumstances described above). By contrast, if the firm has filed a Suspicious Activity Report ("SAR") under POCA or the Terrorism Act 2000, ("Terrorism Act"), disclosing that fact (i.e., the fact of filing of the SAR) will be a 'tipping off' offence.

4.73 Firms may choose to advise the customer/parties to a transaction that concerns as to the effect of the financial sanction may be raised with the Asset Freezing Unit at HM Treasury.

Does a SAR have to be filed?

4.74 Holding an account for a sanctioned party or rejecting or processing a transaction (whether or not in breach of financial sanctions prohibitions) which involves a sanctioned party, is not in itself grounds for filing a SAR under either POCA or the Terrorism Act.

4.75 However, should a suspicion of crime or terrorism arise, firms should consider their obligations under the legislation and whether they should submit a SAR.

Reporting to the FSA

4.76 There is no formal legal requirement to report a true match other than to the Asset Freezing Unit at HM Treasury.

4.77 The FSA has indicated that it regards breaches (not true matches) of financial sanctions to be a matter that would be appropriate for firms to report to the FSA via their usual points of contact. This disclosure should be consistent with the FSA's Principle 11 which requires a firm to "deal with its regulators in an open and co-operative way" and to "disclose to the FSA anything relating to the firm of which the FSA would reasonably expect notice". Firms with a dedicated FSA relationship manager may wish to discuss the practicalities of this as part of their usual supervisory dialogue.

Review customer relationship

4.78 Firms may wish to review their relationship with a customer confirmed as a true sanctions match.

Breaches of Statutory Instruments

4.79 HM Treasury must be informed as soon as practicable where a firm knows or suspects that an offence under any one of the various sanctions has been committed either by itself or by a sanctions target. Failure to do so constitutes an offence.

ANNEX 4-I

Summary of relevant legislation

Note: This summary focuses on legislation relating to terrorism and terrorist financing. Not all country-based regimes are, however, in place for this purpose; some are more human rights based.

United Nations

UNSCR 1373 (2001)

The UN Security Council has passed UNSCR 1373 (2001) which calls on all member states to act to prevent and suppress the financing of terrorist acts. Guidance issued by the UN Counter Terrorism Committee in relation to the implementation of UN Security Council Resolutions regarding terrorism can be found at www.un.org/Docs/sc/committees/1373/

UNSCR 1267 (1999)

The UN has published the names of individuals and organisations subject to UN financial sanctions in relation to involvement with Usama Bin Laden, Al-Qa'ida, and the Taliban under UNSCR 1267 (1999), 1390 (2002) and 1617 (2005). All UN member states are required under international law to freeze the funds and economic resources of any legal person(s) named in this list and to report any suspected name matches to the relevant authorities.

European Union

EC Regulation 2580/2001 as amended

The EU directly implements all UN financial sanctions, including financial sanctions against terrorists, through binding and directly applicable EU Regulations. The EU implemented UNSCR 1373 through the adoption of Regulation EC 2580/2001 (as amended). This Regulation introduces an obligation in Community law to freeze all funds and economic resources belonging to named persons and entities, and not to make any funds, economic resources or financial services available, directly or indirectly, to those listed.

EC Regulation 881/2002 (as amended)

UNSCR 1267 and its successor resolutions are implemented at EU level by Regulation EC 881/2002 (as amended).

The texts of EC Regulations referred to and the lists of persons targeted, are available at
http://ec.europa.eu/external_relations/cfsp/sanctions/docs/measures_en.pdf

UK legislation

The UK has implemented its obligations under UNSCR 1373 under the Terrorist Asset-Freezing Act 2010 (which replaced the Terrorism (United Nations Measures) Orders of 2001, 2006 and 2009). The 2001 and 2006 Orders had been replaced and revoked by the 2009 Order save that directions designating persons under article 4 of the 2001 and 2006 Orders which remained in force on the date of the 2009 Order came into force continued to

apply and the provisions of the 2001 and 2006 Orders continued to apply to such directions.

UNSCR 1267 and its successor resolutions are implemented in the UK by EC Regulation 881/2002 (as amended). The Al-Qa'ida and Taliban (Asset-Freezing) Regulations 2010 provide for penalties of Regulation 881/2002 and, amongst other things, reporting obligations on financial institutions.

Acting under the Terrorist Asset-Freezing etc Act 2010, where HM Treasury has reasonable grounds for suspecting that the person is a person who commits, attempts to commit, facilitates or participates in the commission of acts of terrorism, and it considers the designation necessary for the purposes of protecting members of the public from a risk of terrorism, it can designate that person for the purposes of the Order. This might result in the addition of a name to the HM Treasury list that might not appear on the equivalent UN or EU lists.

A number of organisations have been proscribed under UK anti-terrorism legislation. Where such organisations are also subject to financial sanctions (an asset freeze), they are included on the Consolidated List maintained by HM Treasury.

Regimes currently in place

A list of the financial sanctions regimes currently in place can be found on the HM Treasury website at:
http://www.hm-treasury.gov.uk/fin_sanctions_currentindex.htm

Other regimes

The Department for Business, Innovation and Skills is the UK department responsible for trade sanctions.

Certain trade sanctions regimes, such as those involving an arms embargo, also include measures that place restrictions on the provision of financial assistance related to specific activities, such as military activities.

Below are details of those trade sanctions regimes in effect in the UK, which include restrictions on the provision of finance directly to the prohibited trade activities:

Lebanon

The Counter Terrorism Act 2008

Schedule 7 to the CTA gives power to HM Treasury to issue directions to firms in the financial sector. The kinds of requirement that may be imposed by a direction under these powers relate to

customer due diligence;
ongoing monitoring;
systematic reporting ;
limiting or ceasing business.

The requirements to carry out CDD measures and ongoing monitoring build on the similar obligation under the Money Laundering Regulations. The requirements for systematic reporting and limiting or ceasing business are new.

HM Treasury may give a direction **if one or more** of the following conditions is met in relation to a non-EEA country:

- that the Financial Action Task Force has advised that measures should be taken in relation to the country because of the risk of terrorist financing or money laundering activities being carried on

  (a) in the country,

  (b) by the government of the country, or

  (c) by persons resident or incorporated in the country.

- that the Treasury reasonably believe that there is a risk that terrorist financing or money laundering activities are being carried on

  (a) in the country,

  (b) by the government of the country, or

  (c) by persons resident or incorporated in the country,

  and that this poses a significant risk to the national interests of the UK.

- that the Treasury reasonably believe that

  (a) the development or production of nuclear, radiological, biological or chemical weapons in the country, or
  (b) the doing in the country of anything that facilitates the development or production of any such weapons,
  poses a significant risk to the national interests of the UK.

ANNEX 4-II

Summary of responsibilities for the UK regime

Responsibilities lie with three Government departments and the Financial Services Authority also has a role:

1. The Foreign and Commonwealth Office ("FCO") has responsibility for negotiating in the UN and in the EU on sanctions

2. The Department for Business Innovation and Skills ("BIS") has responsibility for trade sanctions.

3. HM Treasury has responsibility for administering sanctions in the UK, compliance and issuing exemptions to prohibitions by way of licence.

4. The Financial Services Authority ("FSA") has responsibility for ensuring that financial services firms have adequate systems and controls for compliance with the UK financial sanctions requirements.

The FCO

The FCO has responsibility for UK policy in relation to the scope and content of the sanctions regime. The FCO also has responsibility for representing and negotiating the UK's position with respect to the terms of financial sanctions related United Nations Security Council resolutions and European Union Regulations. UNSCRs provide the basis on which the legal sanctions framework is constructed, and EC Regulations give effect to UN obligations in the EU, including in the UK.

The EU can also impose autonomous sanctions within the framework of the Common Foreign and Security Policy.

The FCO maintains a list of current restrictions and information on the countries that are under export controls and sanctions: see www.fco.gov.uk/resources/en/word/doc2/sanctions-regimes

BIS

BIS has responsibility for trade sanctions, setting export controls and administering the FCO list of about 50 countries subject to trade measures. Trade sanctions, such as embargoes on making military hardware or know-how available to certain named countries of jurisdictions, can be imposed by governments or other international authorities, and these can have financial implications. Firms which operate internationally should be aware of such sanctions, and should consider whether these affect their operations; if so, they should decide whether they have any implications for the firm's procedures. Further information and links to lists of affected countries can be found at www.berr.gov.uk/whatwedo/europeandtrade/strategic-export-control/index

BIS also has specific responsibility for implementing United Nations Security Council Resolutions on weapons of mass destruction. Within BIS the Export Control Organisation ("ECO") has responsibility for legislating, assessing and issuing export licences for specific categories of "controlled" goods. This encompasses a wide range of items including so-called dual-use goods,

torture goods, radioactive sources, as well as military items. A licence may be required depending on various factors including the nature of the items exported and any sanctions in force on the export destination.

HM Treasury

HM Treasury is the lead UK Government department on financial sanctions. The key objective of HM Treasury's Asset Freezing Unit (AFU) is to ensure a proactive and effective UK asset freezing regime in partnership with stakeholders. The AFU has four branches, covering Counter-terrorism, International, Licensing and Compliance.

The FSA

The FSA Handbook, in particular Principle 3 and SYSC 6.1.1, places specific responsibilities on firms regarding financial crime prevention. Authorised firms are therefore subject to regulatory requirements relating to the UK's financial sanctions regime.

The following are the specific requirements:

> Principle 3: Management and control
>
> "A firm must take reasonable care to establish and control its affairs responsibly and effectively with adequate risk management systems" and
>
> SYSC 6.1.1
>
> "A firm must establish, implement and maintain adequate policies and procedures sufficient to ensure compliance of the firm including its managers, employees and appointed representatives (or where applicable, tied agents) with its obligations under the regulatory system and for countering the risk that the firm might be used to further financial crime. [Note: article 13(2) of MiFID.]"

Application in law

Sanctions apply in UK law through both EC Regulations and Statutory Instruments (which have been used as the UK's enabling legislation for the application of UN financial sanctions). With regard to EC Regulations, there is direct applicability in EU Member States, so that entities incorporated or constituted under EU law, and persons and entities doing business in the EU (including non-EU nationals) are subject to their provisions. Statutory Instruments apply to any person in the UK and any British citizen, and any body incorporated or constituted under law of any part of the UK (but not subsidiaries operating outside the UK with no UK legal personality). Annex 4-I provides details of international, EU and UK legislation relevant to financial sanctions and asset freezing.

Each Statutory Instrument is unique in terms of detail, restrictions, exceptions, prohibitions the penalties for non-compliance and information requirements.

Who must comply with financial sanctions in the UK?

The relevant Statutory Instruments generally apply to any person in the UK, to any person elsewhere who is a British citizen or subject, and to any body incorporated or constituted under the

law of any part of the UK, although the exact wording may differ from one Statutory Instrument to another. The UK statutory instruments do not apply to subsidiaries operating wholly outside the UK and which do not have legal personality under UK law.

EU Regulations imposing and/or implementing sanctions are part of Community law, are directly applicable and have direct effect in the Member States. The measures apply to nationals of Member States, as well as persons and entities doing business in the EU, including nationals of non-EU countries.

Is it an offence to make funds available to a target of financial sanctions legislation?

This is covered specifically in each relevant Statutory Instrument and EU Regulation. In general terms, any person to whom the relevant legislation applies who, except under the authority of a licence granted by HM Treasury under the relevant legislation makes any funds, economic resources or, in some circumstances, financial (or related) services available directly or indirectly to or for the benefit of persons listed under the relevant Statutory Instrument or EU Regulation is guilty of an offence.

What are the penalties for committing an offence under the legislation?

These are covered specifically in each relevant Statutory Instrument. However, in general terms, any person guilty of an offence under the relevant Statutory Instrument is liable on conviction to imprisonment and/or a fine. The maximum term of imprisonment is currently seven years or two years in the case Statutory Instruments providing penalties for breaches of EU Regulations.

Where any body corporate is guilty of an offence under the relevant Statutory Instrument, and that offence is proved to have been committed with the consent of connivance of, or to be attributable to any neglect on the part of, any director, manager, secretary or other similar officer of the body corporate, or any person who was purporting to act in any such capacity, that person as well as the body corporate is guilty of that offence and is liable to be proceeded against and punished accordingly.

Subscribing to HM Treasury notification service

The Asset Freezing Unit offers a free subscription facility for notification by e-mail when a Financial Sanctions-related release is published on this website and the consolidated list of targets is updated. In order to subscribe, an email should be sent from the email address to be subscribed to AFUsubscribe@hmtreasury.gsi.gov.uk with the words **SUBSCRIBE SANCTIONS** in the subject field, and providing your name, company name, address and telephone number as appropriate.

The BBA alert service

The BBA provides an additional alert service by notifying its members and drawing their attention to amendments published by HM Treasury. The alert service is provided to all BBA member banks and principal contacts.

International requirements

Firms active in non-UK jurisdictions will wish to be aware of the sanctions requirements in each and every country where they operate.

ANNEX 4-III

Summary of Licensing Regime

What is a licence?

A licence is a written authorisation from HM Treasury to allow an activity which would otherwise be prohibited by financial sanctions legislation. The obligations and responsibilities attached to a licence are generally imposed on a sanctions target, but a licence may be issued to a relevant financial institution in order to allow such institution to engage in an activity, such as dealing with funds belonging to a sanctions target, which would otherwise be prohibited. A licence may include associated reporting requirements or other conditions on a financial institution, and these will be made clear in the terms of an individual licence.

Applications to release funds from frozen accounts, or to make funds, economic resources or financial services available to or for the benefit of a sanctions target must be made in writing to the Asset Freezing Unit, HM Treasury, 1 Horse Guards Road, London SW1A 2HQ, or emailed to assetfreezingunit@hmtreasury.x.gsi.gov.uk.

HM Treasury will normally provide guidance letters when issuing licences to banks. Such guidance will specify the purpose for which the licence is being issued, together with any specific obligations on financial institutions including any monitoring requirements.

Operation of frozen accounts under a licence

HM Treasury does not instruct financial institutions on how they should operate frozen accounts that are licensed to permit specific transactions to take place. Some financial institutions operated such accounts by blocking all electronic functionality, or permitting only specified standing orders/direct debits. Other financial institutions allow the accounts to operated without restrictions, but apply specific monitoring. Where accounts are operated openly, financial institutions must ensure that there is sufficient monitoring to satisfy themselves that any breaches by a sanctions target, for example withdrawals in excess of a cash limit stated in the licence, are identified as soon as possible and reported to HM Treasury.

There are primarily four different models by which frozen accounts are operated:

i. frozen accounts of sanctions targets subject to a licence are run as standard accounts with cash cards and full electronic functionality. Monitoring is in place on such accounts to ensure any unauthorised activity by the sanctions target is detected and communicated to HM Treasury without delay.

ii. the original account is frozen and a new account is opened that benefits or other licensed income can be paid into. The sanctions target has no access to funds in the original frozen account. Again, monitoring is in place on such account to detect any unauthorised activity.

iii. access to a cash card is withdrawn. However, the sanctions target is permitted to set up payments, e.g., for rent and utilities, by standing order or direct debit. Remaining funds required (up to a limit specified in the licence) must be withdrawn in person at the

branch counter.

iv. the account is blocked to remove all electronic functionality, and the sanctions target must withdraw cash over the branch counter – there may be a limit on the amount of cash that can be withdrawn, depending on the terms of the licence.

Depending on the model of account operation adopted, there is a balance between ensuring that sufficient controls are in place on such accounts and ensuring that the impact of the asset freezing regime on the individual is not disproportionate.

In respect of the insurance industry, especially general insurance, there may be instances where legitimate third party claims may arise. In such circumstances any payments or services provided may require a licence or amending the current licence. In all instances the advice of HM Treasury should be obtained before any payment is made.

Even where no obligations on a bank are specified in a licence, there are relevant obligations contained in the legislation itself. Part 4 of the 2009 Terrorism Order imposes certain reporting obligations on financial institutions in relation to offences committed under Article 8 and Part 3 of the Order. Where a financial institution is aware of breaches of the asset freeze by a sanctions target, there is a requirement to inform the Asset Freezing Unit as soon as it is practicable to do so. One example is that in a circumstance where a bank is aware, through monitoring of an account, that a sanctions target is in breach of their licence conditions, e.g., through withdrawing more cash than they are permitted, the bank is required by the legislation to inform HM Treasury of the sanctions target's breach as soon as is practicable.

Guidance on, and examples of, General Licences is available on the HM Treasury website at http://www.hm-treasury.gov.uk/fin_sanctions_general_licences.htm.

ANNEX 4-IV

Useful sources of information

UN Security Council: www.un.org/Docs/sc/committees/INTRO.htm.

HM Treasury: http://www.hm-treasury.gov.uk/fin_sanctions_index.htm

FCO: http://www.fco.gov.uk/en/global-issues/counter-terrorism/

Code for Crown Prosecutors: www.cps.gov.uk/publications/docs/code2004english.pdf

Home Office: www.homeoffice.gov.uk/security/terrorism-and-the-law

SOCA: www.soca.gov.uk

European Commission: http://ec.europa.eu/external_relations/cfsp/sanctions/list/consol-list.htm

FSA report on firms' compliance with UK sanctions requirements:
www.fsa.gov.uk/pubs/other/Sanctions%20Final%20Report.pdf

Department for Business Innovation and Skills (formerly Department of Trade and Industry):
http://www.berr.gov.uk/whatwedo/europeandtrade/strategic-export-control/index.ht

US Treasury: http://www.ustreas.gov/offices/enforcement/ofac/programs/

OFAC: http://www.treas.gov/offices/enforcement/ofac/

FATF: www.fatf-gafi.org/

Wolfsberg Group: http://www.wolfsberg-principles.com/

.