AVOIDING THE **PITFALLS**

International sanctions regimes represent a significant compliance challenge, requiring an enhanced approach to standard AML procedures. **Harriet Territt** explains how to avoid inadvertent breach

As the global economy continues to emerge from recession, there is an increasing focus on the role of regulation in maintaining stable financial markets and systems. Concurrently, regulators have signalled a more proactive, intensive approach to supervision and enforcement, for example in the policing of international sanctions, following the announcement of several high-profile investigations and settlements, particularly in the UK and US.

Serious impact

Sanctions are an unusual regulatory creation. Most regulation looks inward, focusing on preventing risky or inappropriate behaviour within an organisation. In contrast, sanctions are a tool of foreign public policy aimed at preventing behaviour condemned by the international community, or encouraging a change of behaviour in a targeted regime. Increasingly, they are used to prevent the financing of terrorism.

The majority of sanctions are multilateral, the general view being that multilateral cooperation is necessary for economic sanctions to be effective. However, notable unilaterally-imposed sanctions regimes exist, such as the US's against Cuba. A common starting point for multilateral sanctions is Chapter VII of the UN Charter, which permits the Security Council to take enforcement measures to maintain or restore international peace and security, including imposing economic, trade or targeted sanctions.

The serious nature of the policy behind international sanctions is reflected in the way they are implemented around the world. A range of specific measures fall under the general heading of "financial sanctions" and they vary in severity and impact – the most comprehensive prohibit any transfer of funds to a sanctioned country and require all assets of a government, corporate entities and residents of the target country to be frozen in jurisdictions where the sanctions are effective. Given the very serious impact of such a comprehensive package on the lives of ordinary people in the target jurisdiction, a more common approach is to put in place targeted asset freezes and/or investment bans on named individuals/entities. These are often combined with export or import bans on certain types of goods and visa bans or travel restrictions.

Variations

The assumption that multilateral sanctions operate identically in every jurisdiction is a common cause of inadvertent breach. Although most multilateral provisions have a common starting point (e.g. a UN resolution), implementation is at a national level and

>>

IN Brief

- The assumption that multilateral sanctions operate identically in every jurisdiction is a common cause of inadvertent breach
- Breaching a sanctions regime is a criminal offence in the UK – maximum term seven years in prison
- A wide range of normal business activities may infringe a sanctions regime
- Enhanced checks and screening are advisable and may offer a defence

variations from the core provisions are not unusual.

For example, in June 2010 the UN Security Council imposed additional sanctions on financial and shipping enterprises relating to "[nuclear] proliferation-sensitive activities" in Iran. The US implemented these via the Comprehensive Iran Sanctions Accountability and Divestment Act and the Iranian Financial Sanctions Regulations, the combined effect of which goes far beyond the UN position, including banning any US government procurement contract being let to a foreign (non-US) company that "exports to Iran technology used to restrict the free flow of information or to disrupt, monitor, or otherwise restrict freedom of speech". This widely drafted provision is capable of affecting many legitimate products, particularly where creative or unexpected use is made of existing software or hardware offerings. In the EU, the European Council also produced a new regulation on 26 July 2010 which implements the UN sanctions but features EU-specific accompanying measures, such as an export block on "dual-use" items; those that have no explicit nuclear or missile-related purpose, but could be used in such processes.

Such variations present a sizable compliance challenge. International financial institutions cannot simply focus on the regime in any one jurisdiction and compliance officers must be familiar with the basic operation in many locations.

> *"EU, US and UK financial sanctions do not distinguish between funds which have been generated by the behaviour at which the sanctions are aimed or 'legitimate' funds"*

Aspects of sanctions regimes can be extra-territorial – for example, the US Patriot Act of 2001 asserts the right of US authorities to "seize funds in non-US banks" so that if tainted funds under the US regime are deposited into an account at a foreign bank, and that bank has an interbank account in the US with a covered financial institution, the funds are deemed to have been deposited into the interbank account in the US. This allows US law enforcement authorities to seize funds in the US account as a substitute for the foreign account.

In the UK, each sanctioned regime is the subject of a separate statutory instrument, based on a relevant EU regulation. Although the UK instruments are broadly similar in format between different regimes, each instrument should be studied carefully as subtle differences can affect what is and is not permitted. Moreover, EU, US and UK financial sanctions are absolute – they do not distinguish between funds which have been generated by the behaviour at which the sanctions are aimed or "legitimate" funds which may be properly due to the payee and entirely unconnected to such behaviour.

Penalties

Breaching a sanctions regime in the UK is treated as a criminal offence with potentially severe penalties – the maximum term of imprisonment for individuals is currently seven years. Directors, managers or senior personnel can also be personally liable if a corporate body is guilty of a breach which can be shown to have been committed with their consent, connivance or neglect.

In 2009, corporate Mabey and Johnson pleaded guilty to breaching sanctions in Iraq and was fined over £3.5m. More recently members of the Royal Bank of Scotland Group were fined £5.6m for failing to have systems and controls to prevent breaches of UK financial sanctions. The US Treasury's Office of Foreign Assets Control (OFAC) has also been active, including settlements with Lloyds TSB which it fined $350m for failure to record prohibited dealings with Iranian and Sudanese customers; and with Credit Suisse Group, which paid a $536m "global" settlement (by far the largest sanctions settlement to date).

The regulators

HM Treasury (HMT) is responsible for the implementation and administration of international sanctions in the UK and is the primary supervisor. HMT maintains the consolidated list of organisations or individuals targeted by the UN, EU and UK, which is regularly updated. Firms must also inform HMT's Asset Freezing Unit as soon as practicable where they have identified an actual match with a person or entity on the HMT list, or where they know or suspect a customer or a person with whom the firm has had business dealings has committed a breach.

The FSA also monitors compliance by financial organisations given its statutory objective to reduce the extent to which an authorised firm can be used for a purpose connected with financial crime. The FSA Handbook requires the implementation of proportionate systems and controls to reduce the risk of a sanctions breach occurring – although there is no specific requirement to report a breach of the financial sanctions regime, Principle 11 requires firms to keep the FSA advised of any relevant issues of which it would normally expect notice.

A wider range

However, the potential impact of the UK regime is wider than this simple, direct prohibition. A form of words commonly used in the relevant statutory instruments creates an additional risk, which is far harder to manage. Often, they provide that no funds or economic resources shall be made available "directly or indirectly, to or for the benefit of" any sanctioned persons. A decision by the English Court of Appeal in 2007 confirms that relevant legal instruments must be construed broadly, and that prohibitions are intended to be draconian in nature.

The prohibition of "indirect benefit" in particular, introduces the possibility that a

Territt: Checks should be updated regularly

wide range of normal business activities can infringe the regime, if the ultimate outcome is that a sanctioned person benefits from them. For example, a sanctioned person who holds shares in a non-sanctioned company which receives a legitimate, substantial payment may receive an "indirect benefit" in the form of increased dividends. Similar issues can arise across the EU and US, given the common derivation of many sanctions from UN resolutions.

Such wording can effectively increase the territorial impact of a sanctions regime. Consider an organisation which has international subsidiaries that are otherwise outside the scope of the US, EU or UK sanctions regimes and can deal with sanctioned persons if no other regime applies. Where the parent organisation (which is subject to a sanctions regime) has a role in directing strategy, providing capital, or can place US/EU or UK nationals on the subsidiary's board, one could argue (on a broad interpretation of the statutory provisions) that it has indirectly caused or permitted the subsidiary to make funds available to sanctioned persons.

Taking care

It is a defence under the UK regime to show that the person did not know and "had no reasonable cause to suspect" that the funds or economic resources were being made available to a sanctioned person. For this reason, enhanced checks – such as screening for indirect as well as direct customers and also third-party payees – are strongly advisable (as noted by the FSA in its 2009 report *"Financial Services Firms' Approach to UK Financial Sanctions"*). If reasonable checks are carried out on major shareholders of, and connected parties to, counterparties and these do not disclose connections to sanctioned persons, the defence will be available. In contrast, the defence may not be available if there is very obvious information available suggesting a connection between a sanctioned person and the direct payee, but this is not investigated.

It is also important to repeat and update checks regularly, particularly to establish that existing clients have not developed obvious connections to sanctioned persons before any transaction takes place and that any clients referred by other authorised firms or persons have been fully screened. This is particularly important in high risk jurisdictions (where sanctioned persons are known to have ties and/or do business). Care should also be taken to adopt a broad approach to sanctions screening, checking for possible misspellings or close name matches.

Harriet Territt is a member of Jones Day's Financial Institutions Litigation and Regulation practice and regularly advises on the application of financial sanctions in the UK
hterritt@jonesday.com

This article first appeared in Issue 1 of inCOMPLIANCE, the publication for members of the International Compliance Association, http://www.int-comp.org/ica. For queries regarding ICA membership, contact Dorinda Gibbons: ica@int-comp.org