THE BANKING LAW JOURNAL

VOLUME 129 NUMBER 6 JUNE 2012

The Banking Law Journal (ISSN 0005 5506) (USPS 003-160) is published ten times a year by A.S. Pratt & Sons, 805 Fifteenth Street, NW., Third Floor, Washington, DC 20005-2207. Periodicals Postage Paid at Washington, D.C., and at additional mailing offices. For subscription information and customer service, call 1-800-572-2797. Direct any editorial inquires and send any material for publication to Steven A. Meyerowitz, Editor-in-Chief, Meyerowitz Communications Inc., PO Box 7080, Miller Place, NY 11764, smeyerow@optonline.net, 631.331.3908 (phone) / 631.331.3664 (fax). Material for publication is welcomed — articles, decisions, or other items of interest to bankers, officers of financial institutions, and their attorneys. This publication is designed to be accurate and authoritative, but neither the publisher nor the authors are rendering legal, accounting, or other professional services in this publication. If legal or other expert advice is desired, retain the services of an appropriate professional. The articles and columns reflect only the present considerations and views of the authors and do not necessarily reflect those of the firms or organizations with which they are affiliated, any of the former or present clients of the authors or their firms or organizations, or the editors or publisher.
POSTMASTER: Send address changes to The Banking Law Journal, A.S. Pratt & Sons, 805 Fifteenth Street, NW., Third Floor, Washington, DC 20005-2207.

Financial and Trade Sanctions: What Banks Need to Know

PETER BURRELL, RITA MITCHELL, AND DAVID SAVELL

The authors discuss the obligations of banks and other financial institutions under the United Kingdom's financial and trade sanctions legislation.

Financial and trade sanctions are used to combat terrorism and to discourage regimes or individuals from acting in ways condemned by the international community or individual nations. Sanctions seek to prevent targeted individuals or entities from dealing with their funds, accessing financial services and trading with specific entities, and are backed by civil and criminal penalties. Compliance is not always straightforward, particularly where different sanctions regimes collide and impose conflicting obligations. This article considers:

- the targets of the U.K. financial and trade sanctions regime;
- what the U.K. financial and trade sanctions prohibit;
- who must comply with the U.K. financial and trade sanctions, including any extraterritorial considerations; and
- practical steps to ensure compliance with the U.K. sanctions.

Peter Burrell is a partner in Willkie Farr & Gallagher LLP and heads the firm's Compliance and Enforcement and White Collar Defense Practices in its London office. Rita Mitchell and David Savell are associates in the firm's Compliance and Enforcement group in London. The authors can be reached at pburrell@willkie.com, rmitchell@willkie.com, and dsavell@willkie.com, respectively.

Published by A.S. Pratt in the June 2012 issue of *The Banking Law Journal.*

The obligation to comply with the U.K. sanctions regime extends to all individuals and entities subject to the U.K. jurisdiction. However, because banks and other financial institutions are most exposed to the risk of breaches under the sanctions legislation, this article focuses primarily on their obligations.

IMPORTANCE OF COMPLIANCE

Recently, the temperature has been rising in the U.K. with the publication of the Financial Services Authority's ("FSA") report on its thematic review of sanctions compliance in April 2009. The review identified widespread failings, especially among small and medium-sized firms, and set the bar for possible future enforcement action in the U.K. in the absence of action to put things right. Following the review, in August 2010, the FSA published the decision notice issued to certain members of the Royal Bank of Scotland Group ("RBS Group"), fining them £5.6 million for failings in their financial sanctions systems and controls.

Most recently, in December 2011, the FSA published its long-awaited financial crime guide, which considers, amongst other financial crime risks, how appropriate governance, risk assessment and screening can prevent businesses from breaching the U.K. sanctions regime.

The most recent U.S. enforcement actions provide an interesting comparison to the way in which the English courts and the FSA, in relation to regulated businesses, view criminal and regulatory penalties:

1. In December 2009, Credit Suisse agreed to pay a U.S.$536 million fine for violating U.S. sanctions against Iran. Settlement papers allege that Credit Suisse systematically hid the identity of its Iranian clients when moving millions of dollars on their behalf. The bank was also accused of helping Libya, Sudan and Burma evade sanctions.
2. In January 2009, Lloyds TSB agreed to pay an unprecedented penalty of U.S.$350 million in lieu of U.S. criminal prosecution for processing prohibited payment transactions made by its clients through non-affiliated U.S. correspondent banks. The extraterritorial aspects of this case should be noted. Lloyds was technically not a U.S. person and none of its actions that caused the prohibited transactions took place in the U.S. However,

Lloyds' actions caused its non-affiliated U.S. correspondent banks to breach OFAC regulations.

3. In 2005 ABN AMRO Bank agreed to pay a U.S.$80 million civil penalty and a fine of approximately U.S.$500 million to settle criminal charges as a result of money laundering and sanctions violations carried out by its New York and Chicago branches. The bank was found to have cleared cheques and processed wire transfers and letters of credit involving Iranian and Libyan parties based on instructions and documents that originated in its Dubai and India branches. As part of the penalty, ABN also agreed to outside audits and the filing of special reports to U.S. authorities for three years.

As a result, it remains vital for companies, especially financial institutions that deal with countless transactions every day, to monitor their compliance with financial sanctions and to seek to ensure that they meet their legal (criminal and regulatory) obligations.

SANCTIONS IN THE EU

The United Nations Security Council is the body responsible for adopting measures which are binding on all UN member states. The EU acts on these measures by adopting a common position and independently adopting sanctions in accordance with the objectives of its foreign and security policy. The UN charter confers upon the Security Council powers to decide in a manner binding for all UN members, restrictive measures required in order to maintain or restore international peace and security, if there is a threat to the peace, a breach of the peace, or an act of aggression.

The EU applies sanctions in pursuit of the specific objectives of the Common Foreign and Security Policy[1] ("CFSP") namely:

- to safeguard the common values, fundamental interests, independence and integrity of the EU in conformity with principles of the United Nations Charter;
- to strengthen the security of the EU in all ways;

- to preserve peace and strengthen international security;
- to promote international cooperation; and
- to develop and consolidate democracy and the rule of law and respect for human rights and fundamental freedoms.

The most frequently applied measures are:

- embargoes on exporting or supplying arms and related materials;
- bans on exporting equipment that could be used for internal repression;
- asset freezes on individuals in government, government bodies or associated individuals;
- travel bans on named individuals; and
- bans on imports of raw materials or goods from the sanctions target.

A large number of the EU sanction regimes are "targeted," meaning the restriction is focused on individual people or organisations, however some EU regimes target all the residents and/or entities of a particular country (e.g. Iran).

The EU sanctions are directly applicable in the U.K. and are therefore effective even before the U.K. brings in an applicable statutory instrument implementing them. When considering any sanctions it is therefore necessary to have regard for both EU and U.K. sanctions and, if a license is required, to consider whether the EU sanctions would permit a license to be granted in those circumstances (see HM Treasury requests and licenses below).

AN OVERVIEW OF THE U.K. FINANCIAL SANCTIONS REGIME

HM Treasury is responsible for implementing and administering financial sanctions in the U.K.. This work is carried out by its Asset Freezing Unit ("AFU"). The FSA has no powers under financial sanctions legislation. However, under its financial crime objective, it has oversight of the systems and controls that regulated firms have in place to reduce the risk of breach of the U.K. financial sanctions regime (see FSA requirements below).

The U.K. sanctions regime targets approximately 2,700 individuals and entities (some of which are resident or based in the U.K.), with the aim of freezing their assets. Although U.K. sanctions can target all the residents and entities of a particular country (e.g. Iran), many of the regimes currently in force target specific individuals and entities (e.g. Al-Qaeda, the Taliban and the Burma/Myanmar regime).

The U.K. financial sanctions regime is made up of a number of different statutory instruments and EU regulations, which implement sanctions imposed by the United Nations Security Council ("UN") and by the EU. Typically, a new statutory instrument is passed in relation to each new group of targets and targets are then added to, or removed from, the list by amending orders.

To help with compliance with the regime, the AFU maintains a consolidated list of sanctions targets in the U.K. This list consists of the names of individuals and entities that have been listed by the UN, the EU and the U.K. under specific financial sanctions legislation. The AFU updates the consolidated list whenever the U.K. financial sanctions regime is updated.

WHAT THE U.K. FINANCIAL SANCTIONS PROHIBIT

One difficulty with the U.K. financial sanctions regime is that there is a different statutory instrument for each group of targets, and the statutory instruments, whilst similar, are not identical. Therefore once a "hit" on the consolidated list is identified, regard should be had to the corresponding statutory instrument to identify the nature of the restriction, the circumstances in which a license could be granted and the relevant reporting requirements. However, there are essentially three offenses:

1. making funds[2] available, directly or indirectly to or for the benefit of a target (the term "listed person" is commonly used to describe sanctions targets);
2. dealing with funds which include other assets owned, held or controlled, directly or indirectly by a target, or a person acting on behalf of a target;
3. participating, knowingly and intentionally, in activities the object or effect of which is:

- to directly or indirectly circumvent the prohibitions on making funds available and dealing with funds; or
- to enable or facilitate the commission of the offenses listed above.

The courts have previously concluded, in a case concerning the payment of benefits to the wives of sanctions targets, that the prohibitions in the legislation were deliberately draconian.[3]

WHO MUST COMPLY WITH THE U.K. FINANCIAL SANCTIONS REGIME?

The obligation to comply extends to any person or entity within the U.K. and any person elsewhere who is a U.K. citizen or an entity incorporated or constituted in the U.K. Overseas branches of U.K. companies are subject to the U.K. financial sanctions regime in addition to any local financial sanctions regime. This is unlikely to give rise to problems within the EU, where the local sanctions regimes are likely to be derived from broadly the same source (the UN and the EU) and, as a result, will target the same people.

Currently foreign subsidiaries of U.K. companies do not have to comply with the financial sanctions regime, however, we may see a change to this in the near future with the U.S. leading the way with its proposed Sanctions Bill which, if passed, will hold U.S. companies liable for business done by their foreign subsidiaries with Iran.

Difficulties can also arise when overseas subsidiaries employ U.K. nationals or book transactions into, for example, London or where overseas transactions result in funds in the U.K. being removed.

Further, the extraterritorial effect of the U.K. financial sanctions regime may well give rise to problems in other jurisdictions. For example, if a branch of a U.K. financial institution takes action required under U.K. law but not required under the law of the jurisdiction in which it operates, it may be liable to its customer. Contractual provisions should be reviewed to ensure that, so far as possible, they guard against this risk by permitting the institution not to comply with a customer's instructions if it could give rise to a breach of any law applicable to the institution and the transaction.

PRACTICAL STEPS TO ENSURE COMPLIANCE

FSA Guidance

There is no positive obligation under U.K. financial sanctions legislation to check whether a customer or a third party is a sanctions target (in contrast to the anti-money laundering ("AML") regulations and the U.S. sanctions regime). A financial institution that does not carry out checks and never deals with sanctions targets will not commit an offense. However, the FSA is likely to take a dim view of this approach in relation to firms it regulates, particularly following the decision notice to the RBS Group in August 2010 (and the recently published financial crime guide in December 2011).

All FSA-regulated firms should pay close attention to the recent guidance (especially the examples of good and bad practice) and the decision notice because they are likely to serve as both a marker for future enforcement action and a benchmark against which compliance will be judged.

Joint Money Laundering Steering Group Guidance

Although there is no explicit obligation to screen customers or transactions, it is obvious from the notices issued by HM Treasury announcing new sanctions and changes to the consolidated list of targets that financial institutions are expected to carry out such checks. The guidance from the Joint Money Laundering Steering Group ("JMLSG"), as amended in November 2009, states that institutions should have an appropriate means of monitoring payment instructions and carrying out checks at the customer due diligence stage.

In practice, there is a clear public interest in enforcing financial sanctions and it is in a financial institution's own interest to carry out checks. This is because:

- the liability for the offenses (see above) is strict under some of the statutory instruments;
- the potential reputational consequences are obvious, and;
- deliberate or continuing failure to screen customers and payment trans-

fers, even where no criminal offense has been committed, is likely to result in regulatory action and might, in an extreme case, lead to the loss of a financial institution's FSA permission to carry on business in the U.K.

To comply with U.K. sanctions, it is recommended that:

- new customers should be screened against the AFU's consolidated list before they are provided with any services or transactions are handled. A target, or agent of one, cannot be accepted as a customer as this will almost inevitably involve dealing with the target's funds. If a sanctions target is identified, a report should be made to the AFU (see below). Existing customers should be checked against the consolidated list. However, the population of sanctions targets is not fixed. As a result, customers need to be screened each time the list is updated. They should also be screened each time there is a change in their details (such as a change in directors or beneficial owners). If an existing customer becomes a sanctions target, its funds should be frozen immediately and a report should be made to the AFU (see below);
- payment instructions should be screened against the consolidated list so that the institution does not process payments to or from targets. If a payment matches with a sanctions target, the instruction should not be acted on and a report should be made to the AFU (see Reporting Obligations below);
- as suggested by the JMLSG guidance,[4] resources should be focused on the areas of business where there is a greater likelihood of involvement with targets, such as direct customer relationships. However, the guidance goes on to warn firms not to ignore low risk areas, for example, where the product or related transaction is not anonymous, its nature is such that it allows for the timely application of CDD measures and the benefits of the product or related transaction cannot be realised for the benefit of third parties. Financial sanctions systems and controls should cover areas where dealings with a target are unlikely, but possible; and,
- firms think about the risks associated with financial sanctions separately from the risks associated with anti-money laundering ("AML"). Whilst

there is overlap between the two, the risks are different as sanctions issues may arise even if the source of the funds is legitimate.

It is also recommended that all firms have adequate systems and controls in place to conduct appropriate risk assessment in relation to the sanctions regime. This will include the following:[5]

- appointing an individual of sufficient authority responsible for adherence to the sanctions regime;
- devising appropriate procedures and policies for financial sanctions screening and treatment of target matches;
- devising appropriate training for staff, and;
- conducting screening on an ongoing basis for all existing and new customers.

Further, extra scrutiny should also be undertaken when Politically Exposed Persons ("PEPs") are banking clients. PEPs are natural persons, outside the U.K., who are or have been entrusted with prominent public functions and immediate family members, or persons known to be close associates, of such persons. Private banks should be cautious when dealing with PEPs and are advised to have ongoing screening and due diligence in place together with annual reviews and enhanced monitoring.

REPORTING OBLIGATIONS

Financial institutions also need to be aware of their reporting obligations under the financial sanctions regulations. If a financial institution identifies an individual or entity as a target on the consolidated list or freezes funds because it suspects that an individual or entity is acting on behalf of a target on the consolidated list, it must report this promptly to the AFU. If a financial institution knows or suspects that an offense has been committed under the U.K. financial sanctions regime, or that a customer or person it has dealt with has breached the regime, it must report to the AFU as soon as possible. The reporting response of a financial institution, on obtaining a match for a target, would be considered by a prosecutor when deciding whether to charge a company or individual with a breach of the sanctions regime.[6]

Regulated firms must also consider their obligation to report to the FSA under Principle 11. The JMLSG guidance states[7] that the FSA has indicated that it would be appropriate for firms to report breaches of financial sanctions (but not target matches) to the FSA.

HM TREASURY REQUESTS AND LICENSES

HM Treasury can request any information that would enable it to ensure compliance with, or detect breach of, the U.K. financial sanctions regime.

Further, HM Treasury can grant licenses exempting particular activities, transactions or types of transactions from the financial sanctions regime. In addition to issuing licenses relating to a specific person, HM Treasury may also issue general licenses which apply to all people designated under a particular regime or regimes.

The obligations and responsibilities attached to a license are generally imposed on a sanctions target, although a license may be issued to a relevant financial institution. By way of example, Bank Sepah International is a target of U.K. sanctions against Iran, but has been granted a license (subject to independent monitoring) to permit it to make certain payments.

There are separate offenses of refusing or failing, without reasonable excuse, to comply with any request made and/or breaching the conditions of a license, and/or knowingly or recklessly providing false information in obtaining a license.

INTERACTION WITH THE U.K. AML REGIME

It is important to bear in mind the relationship between the U.K. financial sanctions regime and the U.K. AML regime. If, for example, a transaction concerns an individual who is subject to financial sanctions because of suspected involvement in terrorism, there are likely to be obligations to report under both the sanctions regime (see above) and the Proceeds of Crime Act 2002 (“POCA”) or Terrorism Act 2000 (“TA”) (reporting to the Serious Organised Crime Agency (“SOCA”)).

There is no clear hierarchy between the financial sanctions and the AML regimes, but making a disclosure that may prejudice an investigation into terrorism or money laundering is an offense ("tipping off") under POCA (s333) and/or TA (s21D). As a result, it may be prudent in sensitive cases to report first under POCA or TA to SOCA, confirming an additional intention to report to the AFU. If assets are frozen it may also be necessary to tell the customer. Tipping off is generally not an issue under the financial sanctions regime itself because the names of those targeted by the regime are publicly available. However, there are circumstances where a firm is required to keep confidential the fact that someone, or an entity, is the subject of sanctions, and breach of this requirement is a separate criminal offense.

DEFENSES

Where liability is not strict, the defense to an allegation of breaching the sanctions regime is generally that the person did not know, and had no reasonable cause to suspect, that he was dealing with the funds of a target or making funds available to one.

In our view, given HM Treasury's notices, the JMLSG guidance and the FSA's requirements, financial institutions will need to show that they took proactive steps to check whether their customers and third parties were targets before the defense will be available to them. There may be a balance to be struck based on the costs and practicalities of screening versus the potential risk that a particular customer is, or a particular transaction may involve, a sanctions target, but doing nothing is simply not viable.

Importantly, there is no de-minimis level below which financial institutions are not required to carry out checks.[8]

PENALTIES FOR NON-COMPLIANCE WITH THE SANCTIONS OFFENSES

The maximum penalty in the U.K. for a financial sanctions criminal offense is imprisonment for seven years and/or an unlimited fine. Where the offense has been committed by a company and is shown to have been committed with the consent or connivance, or because of the neglect, of a director, manager, secretary or similar officer, that person is also guilty of an offense and can be imprisoned or fined.

Under POCA, the courts also have powers to confiscate assets obtained as a result of criminal conduct.[9] In the case of financial institutions this would be the fees and other funds received from the sanctioned entity. In the case of a company it may be anything up to the full value of the contract, although in recent cases arising from the Iraq "Oil for Food" investigations, the courts have stopped short of such a draconian approach.

In addition to this, a firm that breaches U.K. financial sanctions is also at risk of FSA enforcement action.

FSA ENFORCEMENT ACTION

The basis of any enforcement activity by the FSA in this area may be Principle 3 of the FSA's Principles for Businesses ("PRIN") and rules 3.2.6 and 6.1.1 of the Senior Management Arrangements, Systems and Controls sourcebook ("SYSC"), which require firms to have effective systems and controls to counter the risk that the firm might be used for the purposes of financial crime. However, enforcement against RBS was contrary to Regulation 20(1) of the Money Laundering Regulations 2007, which requires firms to have in place appropriate, risk-sensitive policies and procedures to prevent activities relating to money laundering and terrorist financing.

NOTES

1 Set out in Article 11 of the Treaty on EU

2 "Funds" include cash, all kinds of payment instruments, deposits, shares, derivatives, interest, guarantees, letters of credit and rights of set-off.

3 *R (M and others) v. HM Treasury* [2007] EWCA Civ 173

4 See paragraph 4.19 of Part III of the guidance.

5 Chapter 3, Financial services firms' approach to UK financial sanctions.

6 See, the Code for Crown Prosecutors.

7 See paragraph 4.77 in Part III.

8 Chapter 1, page 6, Financial services firms' approach to UK financial sanctions.

9 POCA, Part II.