FINANCIAL AND TRADE SANCTIONS BRIEFING II – UK AND EU

Particular issues requiring careful consideration for those subject to the UK and EU sanctions regimes

Introduction

In our previous sanctions briefing, we gave an introduction to the UK and EU financial sanctions regimes. In that briefing, we indicated that in a number of areas we would return to the issues we had raised and explore them in more depth. We aim to do so in this briefing before turning in later briefings to a summary of the position in the US and a short compare and contrast between the US and UK financial sanctions regimes.

Since our first briefing, particular focus has had to be paid to the risks of financial institutions becoming involved in "indirectly financing" Iranian interests contrary to EU and UK sanctions. We therefore consider this further below because it raises particular issues when it comes to due diligence and knowing your customer's business.

Particular jurisdictional issues arising under the UK and EU sanctions regimes

In our previous briefing, we commented that overseas branches of UK companies are subject to UK financial sanctions in addition to any local financial sanctions regime. However, the position was not the same as regards overseas subsidiaries of UK companies, which may only be subject to local law. However, any financial institution which conducts business on a global basis will need to consider carefully the extent to which it is appropriate to exempt locally incorporated subsidiaries from complying with the UK and EU sanctions regimes. This can give rise to a number of difficulties.

First, to the extent that those overseas subsidiaries employ UK nationals, those UK nationals will be subject to the UK and EU financial sanctions regimes and will therefore have to comply with them. This could mean that either they inadvertently commit a criminal offence because they have received inadequate training on the latest changes to the UK or EU financial sanctions regimes or, alternatively, they have to be removed from any involvement in the transaction. On a number of occasions in the past, we have had to advise clients that transactions which were to take place totally overseas needed to be restructured to ensure that no UK persons were involved. This can be particularly difficult when line managers are UK nationals since they may also be exposed to potential criminal offences through failing to stop transactions for which they would otherwise be responsible. Simply seeking to remove themselves from the deal or transaction is therefore not sufficient in all cases.

Secondly, those overseas subsidiaries will need to be careful to ensure that no aspect of the transaction touches the UK, thereby triggering an offence by a third party. It is possible for someone overseas to be exposed to UK criminal liability if their actions overseas cause an offence to be committed in the UK.

In a number of situations we have seen, transactions have originated in Asia but the relevant accounting entries have been made in London where the revenue is then recognised. Where the UK financial institution is profiting from the activities of its overseas subsidiaries, the activities of the overseas subsidiary could trigger criminal offences by the entity into whose books and records the transactions are booked. In those circumstances, the overseas subsidiary as well as the UK company itself could face criminal prosecution. Therefore, unless those responsible for booking transactions recognise the potential sanction sensitivities, it would be unwise to exempt overseas subsidiaries from compliance with the UK or EU sanctions regimes.

In addition to guarding against potential criminal liability, financial institutions are expected to have systems and controls in place to mitigate the risk that the firm will be used in furtherance of financial crime. The Financial Services Authority's ("FSA") expectations are embodied in the FSA Handbook SYSC 3.2.6R and 6.1.1R. Where overseas subsidiaries are undertaking transactions which the UK financial institution could not itself undertake and where revenues from those transactions are flowing either directly, through book-keeping, or indirectly through dividends or global treasury operations, into the UK institution, the FSA may be able to argue that in those circumstances any exemption given to the local subsidiary means that the firm's systems and controls are inadequate.

Where a financial institution does decide to operate a single global sanctions standard, then it is vitally important to ensure that any contractual commitments to clients are modified accordingly. We have advised clients in situations where the UK institution has contractual language which entitles it to refuse to process transactions across an account, where to do so would put it in breach of the UK or EU sanctions regime. However, such clauses would not offer any protection to an overseas subsidiary which itself may not have been committing any criminal offence under English law or otherwise be in breach of EU sanctions but which has the direct client facing relationship and therefore contractual commitments. Any deficiency in the contractual wording can be remedied simply by inserting language to the effect that the local subsidiary will not carry out any transactions or process any instructions which would put it or any group company in breach of any applicable law or regulatory requirements, including English law. It is also worth including language in the clause which means that English law is deemed to apply to the overseas' subsidiaries, even if in reality it does not.

The extent of due diligence

In our previous briefing, we highlighted that there is no express requirement under the FSA's SYSC to screen either customers or transactions against the relevant lists. However, the Joint Money Laundering Steering Group's ("JMLSG") Guidance states that institutions should have an appropriate means of monitoring payment instructions and carrying out checks at the customer due diligence stage. In our earlier briefing, we also set out our own views as to why financial institutions should undertake such checks. However, the critical issue is "on whom"?

The FSA's expectations in this area have increased over time. For example, those who are reliant upon automated systems should ensure that those systems can make "fuzzy matches", ie, they are able to identify similar spellings of names and should not restrict their search to exact customer names only.

For those whose customer base includes corporates, the FSA's expectation is that both directors and beneficial owners should be screened. The issue then is, what is meant by "beneficial owner". For these purposes, the expectation is not that just those owning more than 25% of the share capital should be screened against the relevant list, but any beneficial owner which is identified at the time of the customer on-boarding process or thereafter as part of the ongoing monitoring of the customer. Of course, having checked those names against the relevant list at the time of on-boarding, it is also necessary to re-check those names as part of the ongoing monitoring of the account. Systems therefore need to be devised such that where screening against the list becomes automated, it is not just the customer name but also the names of relevant directors and beneficial owners which are included within the population of names which are subject to screening/checking.

The importance of due diligence on a client or customer's business has never been greater, given the breadth of some of the sanctions regimes, in particular the Iranian sanctions. For example, under Article 5 of EU Council Regulation No. 267/2012, it is prohibited to provide, directly or indirectly, financing or financial assistance related to the goods and technology listed in the Common Military List or in Annex 1 or 2 to the EU Regulation. That includes loans for any sale, supply, transport or export of such items.

The following example demonstrates the breadth of Article 5. A bank which provides an overdraft facility to a company involved in the export of such goods to Iran may be infringing Article 5, particularly if the overdraft is used to meet the costs of exporting the goods eg, to pay for freight. Unless the bank has done due diligence on the nature of the customer's business, it may not appreciate this risk. After all, the sanctions apply, even though the customer is a UK company, has no other obvious connections to Iran and is not on any sanctions list.

There are similar offences under other articles of the EU Regulation, for example: Article 5, paragraph 2(b) (relating to the goods and technology referred to in Annex III); Article 9 (relating to the goods and technology referred to in Annex IV); Article 11(1)(d) (relating to the import, purchase or transport of crude oil and Iranian petroleum products); Article 13(1)(d) (relating to the import, purchase or transport of petrochemical products of Iranian origin); and Article 15(1)(c) (relating to the sale, supply, etc. of precious metals and diamonds). To prevent the commission of any of these offences, much greater due diligence will be required on customers and their businesses.

It is therefore no longer sufficient to screen customer names and those persons associated with the customer, but also the counterparties with which they are dealing. On a risked based approach it will also be necessary to understand the nature of the client's business. Higher risk customers will include those who are involved in the petrochemical or oil and gas industries or in the trading of precious stones.

Reporting obligations

In our previous briefing, we highlighted the various reporting obligations which can arise when dealing with those on sanctions lists.

When considering your reporting obligations, it is important to recognise at the outset the different reasons why an entity may appear on a sanctions list. That can be for a number of reasons:

- the individual is suspected of being involved in terrorism;
- the individual or entity is subject to asset freezing financial sanctions;

Of course, with respect to some sanctions regimes, in particular, those regarding Iran and Syria, the sanctions are not limited to those who are on the proscribed lists, but apply more widely. So, for example, in the case of Syria, the restrictions on insurance or reinsurance apply to any company owned by the Syrian Government.

In addition to the financial sanctions, as outlined above, trade sanctions apply to activities and are not specific to particular named entities or nationalities.

Each of these scenarios gives rise to slightly different reporting considerations.

Those suspected of being involved in terrorism

Where a financial institution suspects that a customer or putative customer is on the proscribed list because of links to terrorism and it has information which relates to the whereabouts of the assets of that customer, then the financial institution will need to consider whether the money laundering offence under section 18 of the Terrorism Act 2000 is applicable or one of the other offences under the Terrorism Act 2000, for example, fund raising (section 15), use and possession of terrorist property (section 16) or being involved in funding arrangements (section 17). If any of those offences are applicable, then the financial institution will need to consider its duty to make a report under section 21A of the Terrorism Act 2000. That report will of course be made to SOCA as a "Suspicious Activity Report" with the "Terrorism Act" box ticked on the relevant form.

In addition to considering the reporting obligations under the Terrorism Act 2000, the financial institution should also consider its obligations to make a report under the Proceeds of Crime Act 2002 ("POCA"). The money laundering offences under POCA are potentially broader than the money laundering offence under the Terrorism Act 2000, particularly since section 329 of POCA means that "money laundering" is committed by the simple possession of the proceeds of criminal conduct. Of course a terrorism offence would constitute "criminal conduct" for the purposes of POCA and if funds have flowed from that offence, section 329 is likely to apply. A reporting obligation may therefore arise under section 330 of POCA and for the Money Laundering Reporting officer ("MLRO") under section 331 of POCA.

A financial institution will also need to consider whether the potential transaction is one which requires consent, either under the Terrorism Act 2000 (section 21ZA) or under POCA (section 338).

In addition to reporting suspicions of substantive offences, either under the Terrorism Act 2000 or POCA, institutions will also need to consider any reporting obligations under the relevant statutory scheme which may have lead to the person becoming designated.

For example, the Terrorist Asset-Freezing etc Act 2010 replaced, amongst other legislation, the Terrorism (United Nations Measures) Order 2009 and the Terrorist Asset-Freezing (Temporary Provisions) Act 2010. It makes provisions for imposing financial restrictions on, and in relation to, certain persons believed or suspected to be or to have been involved in, terrorist activities. Under section 19 of that Act, a relevant institution must inform the

Treasury as soon as practicable if it knows or has reasonable cause to suspect that a person is a designated person or any person has committed any offence under any provision of Chapter 2 of that Act. The reporting obligation only applies if the information or other matter on which the knowledge or suspicion is based came to it in the course of carrying on its business.

Not only is the place of reporting different, the report has to be made to the Treasury rather than SOCA, but the information which is required to be disclosed is also different and is set out in the statute. The Terrorism Act 2000 requires the information or other matters on which the knowledge or suspicion is based and any information the institution holds about the person by which the person can be identified to be reported. In addition, where that person is a customer of the institution, the institution must also state the nature and amount or quantity of any funds or economic resources held by it for the customer at the time when it first had the knowledge or suspicion. That reporting obligation arises irrespective of whether the financial institution considers that those funds or economic resources come from terrorist or lawful activity.

It is also worth highlighting that the reporting obligation arises where the institution suspects that an offence has been committed, either by the designated person or by another person, in this case, under the Terrorist Asset-Freezing Act 2010. In some circumstances, that may require the financial institution to report itself to the Treasury for having committed an offence. We have advised financial institutions in similar situations, for example, where the institution has undertaken transactions on behalf of a designated individual, where they did not "know" that the individual was designated but where they had reasonable cause to suspect that they were and they dealt with the funds or economic resources of that person. The offence can therefore be committed even though the financial institution had no actual knowledge or subjective suspicion about its customer. This is because the test under the various offences is an objective one, namely, having "reasonable cause to suspect".

Finally, where the institution does suspect that it has been involved in a breach of the relevant prohibitions, then the institution is almost bound to report that to the FSA in accordance with Principle 11.

Reporting under the Financial Sanctions Regimes

We have summarised above the potential reports which may be required in the context of terrorism related suspects. With respect to those individuals or entities who are "designated" on the sole ground that they are from rogue regimes, it is perhaps unlikely that the reporting obligations in the Terrorism Act 2000 will arise.

Nevertheless, the institution will still need to consider the relevant statutory regime enshrining the financial sanctions as most of these contain their own reporting obligations.

For example, the Zimbabwe (Financial Sanctions) Regulations 2009 provide for the freezing of the assets of various individuals [and/or entities] associated with Robert Mugabe. The schedule to those regulations requires a relevant institution to report to the Treasury if it knows or suspects that a relevant person is a designated person or has committed an offence under Regulations 6, 7, 9 or 10 of that statutory instrument. Similarly to the provisions under the Terrorism Act 2010, the schedule also specifies the information to be reported to the Treasury.

Of course, if the institution suspects that an offence has been committed under the sanctions regime, then it will also need to consider, in addition to its reporting obligations to the Treasury, whether any of the reporting obligations under POCA arise. For example, if the suspicion is that a designated person has dealt with their assets which should otherwise have been frozen, then the institution will need to consider whether a report should be made under section 330/section 331 of POCA.

Reporting in respect of export controls

As stated above, in addition to the financial sanctions regimes, transactions can be subject to trade sanctions as well. Where trade sanctions apply, licences may need to be applied for before the relevant transaction can take place. Of course, if a financial institution suspects that a customer is acting in breach of relevant trade sanctions, then it will need to consider its reporting obligations under POCA (as summarised above). Similar reporting obligations to the FSA and the Treasury also apply to trade sanctions.

There are also distinct reporting obligations under trade sanctions which provide exemptions to the prohibitions. In relation to The Export Control (Iran Sanctions) Order 2012, it is prohibited to be knowingly concerned in an activity prohibited by Article 11(1)(b) – (d) of EU Council Regulation No. 267/2012, which relates to the purchase, import or transport (or financial assistance or the provision of (re)insurance relating to those activities) of Iranian Crude Oil or Petroleum Products. The EU regulation provides exemptions to performing duties under trade contracts up to 1 July 2012 providing that the person seeking to perform the contract has notified HMT at least 20 days in advance of the activity or transaction. Getting these reporting obligations wrong could constitute a criminal offence. Similar notification requirements in respect of trade sanctions are applicable to Syria (EU Council Regulation No. 36/2012).

In summary, when financial institutions come across sanctions issues, they need to consider very carefully their reporting obligations. In some cases, reports may be required to SOCA under both the terrorism legislation and POCA. Reports are also likely to have to be made to the Treasury.

Conclusion

As can be seen from the above, the financial sanctions regimes are onerous and have far-reaching effects. Financial institutions will need to consider carefully the extent of their customer and transaction due diligence to ensure that they remain compliant with the sanctions regimes. Coupled with the additional reporting obligations, this is an area of increasing risk.

In our next briefing, we will look at US sanctions and how they can apply directly to UK-based financial institutions as well as to US employees working within those institutions.

* * * * * * * * * * * * * * *

If you have any questions regarding this memorandum, please contact Peter Burrell (+44 207 153 1206, pburrell@willkie.com), David Savell (+44 207 153 1204, dsavell@willkie.com), Rita Mitchell (+44 207 153 1214, rmitchell@willkie.com), Danielle Black (+44 207 153 1228, dblack@willkie.com), or the Willkie attorney with whom you regularly work.

Our London office is located at City Point, 1 Ropemaker Street, London EC2Y 9HT, England. Our telephone number is +44 20 7153 1229 and our facsimile number is +44 20 7153 1115. Willkie Farr & Gallagher LLP is headquartered at 787 Seventh Avenue, New York, NY 10019-6099. Our telephone number is (212) 728-8000 and our facsimile number is (212) 728-8111. Our website is located at www.willkie.com.

August 23, 2012