TFR
TRADE & FORFAITING REVIEW

A Guide on Financial Crime Prevention in Trade Finance

GENERAL EDITORS: NEIL CHANTRY, ROSALI PRETORIUS, AND THIERRY SÉNÉCHAL

Wilmington

A Guide on Financial Crime Prevention in Trade Finance

is published by Ark Group in association with Trade & Forfaiting Review

ark GROUP
A Wilmington Company

TFR
TRADE & FORFAITING REVIEW

EUROPE OFFICE
6–14 Underwood Street
London N1 7JQ
United Kingdom
Tel +44 (0)207 566 5792
Fax +44 (0)207 324 2373
publishing@ark-group.com

ISBN: 978-1-78358-169-6 (hard copy)
978-1-78358-170-2 (PDF)

Head of Content Strategy
Fiona Tucker
fiona.tucker@wilmington.co.uk
Reports Content Manager
Helen Roche
helen.roche@wilmington.co.uk
Assistant Editor
Laura Slater
laura.slater@ark-group.com
Marketing enquiries
Irene Pardo
irene.pardo@wilmington.co.uk

TFR0001

TFR
TRADE & FORFAITING REVIEW

A Guide on Financial Crime Prevention in Trade Finance

GENERAL EDITORS: NEIL CHANTRY, ROSALI PRETORIUS, AND THIERRY SÉNÉCHAL

Wilmington

Contents

Executive summary

TRADE FINANCE is a vital component in maintaining a competitive and productive global economy. Approximately 80 per cent of the world's current US$20trn of trade flows is financed by some form of trade credit. An unfortunate by-product of the success and abundance of such trade activities, however, is its attraction to perpetrators of financial crime. This is an issue of global significance, and the work being undertaken to combat abuse of trade finance activities by criminal and terrorist interests is of paramount importance.

Trade finance has been an area of growing attention in past years, and the Financial Action Task Force (FATF), the Wolfsberg Group, and the Joint Money Laundering Steering Group (JMLSG) in particular have drawn attention to the misuse of international trade finance as one of the ways criminal organisations and terrorist financiers move money to disguise its origins and integrate it into the legitimate economy. Business organisations such as the International Chamber of Commerce (ICC) have consistently voiced strong public support in favour of improving the resilience of the banking sector and combating financial crime and money laundering activities. It has also provided practical support from its anti-crime arm, ICC Commercial Crime Services (CCS).

What is it that makes trade finance a particular target for these criminals? The problem exists in the fact that the very nature and complexity of trade finance transactions, and the huge volume of trade flows that exist, can hide individual transactions and help criminal organisations to transfer value across borders. As a result of this, every organisation involved in trade finance holds responsibilities with regards to the prevention of financial crime. This report covers the various aspects of financial crime in relation to trade finance, and it outlines the various areas targeted by financial crime and the associated risks. Drawing on the experience of recognised experts in the trade finance sector, the report provides practical guidance on the specific financial crime risks in trade finance, and offers advice on the preventative measures that can be taken.

Chapter 1 provides the background information on financial crime in relation to trade finance. It outlines the vulnerabilities of trade finance to criminals and the need for stringent efforts to combat financial crime. The chapter provides detailed information on the latest global trade finance data

and the wider danger to the global economy of too much de-risking in the global financial marketplace.

Chapter 2 moves on to discuss the proper integration of compliance into successful trade finance. It provides in-depth advice on categorising trade finance and developing a risk appetite, and important guidance on the allocation of responsibilities to deal with financial crime risks. The chapter includes information on building the architecture of a sound and business-friendly financial crime risk strategy within an organisation, with detailed advice on: risk assessments; policies and procedures; due diligence; governance; and training and awareness.

Fraud in trade finance is the focus of Chapter 3. This section of the report reviews the specific risks and examples of fraud involving the use of trade and commodity finance instruments. It identifies how vulnerable banks can be to fraud when loans are secured on commodities and references the Quingdao Port scandal, and it suggests some practical approaches to fraud prevention. Included in the chapter is a detailed explanation of the principles of a letter of credit and the fraud exception rule.

Chapter 4 tackles the topic of money laundering, with a specific focus on the offences and obligations relevant to the trade finance sector. The chapter explores the methods of money laundering used in the trade finance world, and provides expert advice on the preventive measures which can be taken to counter money laundering in trade finance.

Terrorism financing is another area of financial crime related to trade finance, and this is covered in Chapter 5. This chapter outlines the terrorism financing offences related to trade finance and the obligations relevant to the trade finance sector. It provides examples of terrorism financing through trade and the requisite measures to prevent such activities.

Chapter 6 covers sanctions concerns in trade finance, and it explains what sanctions may be relevant in the trade finance sector in particular jurisdictions. It assesses the impact and practical application of sanctions and considers what trade finance firms can do to protect themselves. The chapter also provides a checklist of activities which are key to any sanctions compliance and protection programme.

The report is aimed at a broad spectrum of individuals and organisations involved in different components of the cross-border trade transaction chain. Specifically, the report will prove helpful to those involved in the financing of trade – although exporters and importers will also find it a useful guide. The readership therefore comprises: trade bankers, compliance officers, corporate treasurers/CFOs of commodities companies, and other exporters and importers, vendors, consultants, and legal advisers. Regulators will also find it useful as a barometer of how their requirements are being interpreted and put into practice.

Foreword

DURING THE course of the three years I have been at the TFR helm, the symbiotic relationship between trade and the credit that finances it has been something we have celebrated through our news, case studies, and in-depth features. It is a very special relationship, but it has come under attack on a number of fronts.

The global financial crisis caused the steepest contraction of world trade volume since the Great Depression in the 1920s and damaged economies which had depended on exports for their growth. Were it not for initiatives such as former WTO director general Pascal Lamy's Expert Group for Trade Finance that helped start projects to remove obstacles to co-risk sharing and co-financing, trade finance could well have dried up altogether.

But the industry came together, found solutions, and demonstrated how well financial institutions can pull together in a crisis. One of the legacies of that crisis has been the increase in financial crime regulation. There is no evidence that there are suddenly more financial crime perpetrators or more misappropriate funds – but regulators are certainly jumpier. One can understand them adopting a belt and braces approach to protecting financial systems, but the unintended consequence of all of this has been further contraction in trade finance activity. Sometimes it is easier just not to do the deals at all than put in place all the measures necessary to avoid censure.

Again the industry has come together with projects such as the SWIFT KYC Register, and it falls to the financial institutions to share their knowledge and best practice so that proportionate safeguards fight crime but do not damage trade.

This report sets out the scope of the financial crime regulatory framework in practical, transactional language, and it aims to promote a wider understanding of what the requirements mean on the ground. I am grateful to our expert contributors for all their hard work.

Clarissa Dann
Editor
Trade & Forfaiting Review

About the general editors

Neil Chantry

Neil is global head of policy and compliance, trade and supply chain, global transaction banking, HSBC, UK. Neil joined the HSBC Group in London in 1972, initially working with the British Bank of the Middle East in Dubai and Ras-al-Khaimah in the UAE, Oman, Bahrain, and Djibouti until 1980, when he went to Hong Kong. Various postings in Hong Kong and Pakistan followed until in 1994 he transferred to the UK to HSBC Holdings plc, the head office of the HSBC Group.

Since 1973, Neil has spent the majority of his time managing various import and export departments, running and developing executive training courses for trade and foreign exchange, as well as working with business users and the Group's IT developers in the specification and design of many of the trade support systems used by the HSBC Group. Today, Neil is responsible for the formulation of policy and the maintenance and introduction of best practice procedures for Trade Services Operations for the HSBC Group, and for the development of compliance related processes.

Neil has been a representative of the UK delegation to the ICC Banking Commission since 1994, and was a member of the eUCP Working Group. He has worked with the SWIFT TSAG Scoping Group and was a member of the Trade Services Utility Customer Requirements Group and Rules Group, and the SWIFT/ICC B.P.O. Rules Drafting Group.

Neil is currently head of the ICC Commission on Banking Techniques and Practice Executive Committee, Chair of the Commission Compliance Group, and Chair of the ICC UK's Banking Committee. He is also the chair of the Wolfsberg Group's Trade Group working on trade specific guidance to Wolfsberg members related to the application of various regulatory requirements for NPWMD, AML, sanctions, and anti-terrorist finance.

Rosali Pretorius

Rosali leads Dentons' London-based financial services and funds practice. She focuses on exchange traded and OTC commodity and other derivatives, alternative investment funds, and the financial regulation of these and other products. Acting for banks, broker-dealers, fund managers, insurance

companies, and other financial intermediaries, she advises both sell-side and buy-side clients.

Rosali read law in South Africa and England. After short stints as a precious metals analyst in Johannesburg and as law lecturer at King's College London, she joined Dentons as a trainee in 1995. Rosali was shortlisted for 'The Lawyer's Assistant Solicitor of the Year Award' in 2001. In 2006 she was seconded to the legal department of Goldman Sachs, focussing on commodity and funds derivatives.

Commended in *Lawyer Monthly* 'Women in Law Awards' which celebrate and highlight the achievements of women in the legal profession across the globe, she is a popular speaker on financial services regulation and a regular contributor to *TFR*.

Thierry Sénéchal

Thierry Sénéchal is senior policy manager of the banking commission at the International Chamber of Commerce (ICC). He has 20 years of experience in financial crime risk, in both investigative and policy functions, in the public and private sectors, and across a wide range of topics (AML, sanctions, financial fraud, and insurance claims). As senior policy manager of the banking commission at the ICC, he leads and coordinates the efforts to develop industry standards in banking and financial services, including the policy guidelines on financial crime risks.

He is one of the initiators and a founding member of the ICC AML Task Force in 2008. Prior to joining ICC, Thierry Sénéchal served as executive director, financial audit and policy with the Mazars Group, a leading international accountancy firm of 14,000 professionals in 70 countries (2002–2005). At Mazars, he led a wide range of client engagements for financial institutions, central banks, regulators, and government treasuries around the globe, including AML compliance audits, financial investigations on misuse of public funds, and evaluation of government budgets.

Before joining Mazars, he served as an international civil servant with the UN Security Council for which he handled the investigation of a US$350bn claim programme and overall responsibilities for the review of the banking and financial claims arising out of the invasion of Kuwait by Iraq. He started his career as financial fraud and asset recovery investigator with Seri Expert-McLarens.

About the authors

Clarissa Dann
Clarissa is editor of *Trade & Forfaiting Review* (*TFR*), the specialist trade and receivables finance information service which is now in its 18th year. *TFR* includes a monthly magazine, an online information service, industry events, reports, and two annual awards competitions. Clarissa's former roles included running legal and regulatory publishing teams at Thomson Reuters and Lexis Nexis before she completed her MBA in 2004 from Cass Business School in London and re-trained as a financial journalist. Based in the UK, she is regular participant in and reporter on trade and commodity finance events around the world, and she is currently studying for the Certificate in International Trade Finance (CITF). You can follow Clarissa at twitter.com/clarissadann.

Sean Edwards
Sean is an English solicitor, formerly with Clifford Chance, and is now head of legal at Sumitomo Mitsui Banking Corporation (SMBC) Europe Limited. He is Deputy Chairman of the International Trade and Forfaiting Association (ITFA) and Chairman of the ITFA Market Practice Committee. He was a member of the drafting group of the Uniform Rules for Forfaiting (URF 800), a co-operative initiative of the ITFA and ICC and published by the ICC. Sean has written articles on forfaiting for all the major trade finance magazines and he is on the editorial board of *Trade & Forfaiting Review* (*TFR*). Sean has an honours degree in law from Bristol University.

Imogen Holmgren
Imogen graduated at the University of Poitiers, France in Public Law and is a trainee solicitor in the Trade Finance team of the Energy & Natural Resources Group of Reed Smith. She joined the London office of Reed Smith in 2013 after having worked originally in Reed Smith's Paris office.

Robert Parson
Robert is a partner in the Energy & Natural Resources Group of Reed Smith, based in the London office. He graduated in Law at Sheffield University and, after spending the early part of his career with Reed Smith's London Legacy

Commodity practice at Richards Butler, he built a strong reputation as a partner in one of London's best-known trade law firms before rejoining Reed Smith in 2008.

He focuses on the financing of international trade and commodities, acting for many of the world's major commodity banks, traders, exporters, and other participants in the global trade market, and he advises regularly on structured trade finance deals, international payments, letters of credit and guarantees, and supply chain finance solutions. Robert is named in the current editions of Legal 500 and Chambers as a leading individual. He is the editor of the legal journal *Finance & Credit Law*.

Christina Pope

Christina is a trainee in Dentons' financial services and funds group. On graduation, Christina worked for Kroll in the legal technology business, and then joined Dentons as the senior paralegal and manager of litigation support in the dispute resolution department. Christina has completed a Masters in Law, which included an elective in Financial Regulation and Compliance.

Emma Radmore

Emma is a managing associate in Dentons' London-based financial services and funds practice. She advises on all aspects of regulation under financial services legislation, and her client base includes UK, European, and international firms, both within and outside the regulated sector. Her main areas of focus are advising on structure of business to obtain the best financial regulatory treatment, the scope of the authorisation requirement under the Financial Services and Markets Act 2000, and helping clients to obtain authorisation, drafting client take-on documentation, and advising on compliance with regulatory requirements. She advises clients in all parts of the financial sector, including banks, insurers, asset managers, and intermediaries, with a focus on the retail markets.

A large part of Emma's practice involves advising clients on policies and procedures to counter financial crime. She advises regulated and unregulated firms on anti-money laundering requirements, the financial sanctions regime, and the prevention of bribery and corruption. She has advised clients in all industry sectors on the impact of the Bribery Act 2010 on their businesses, and she has given training, drafted high-level principles, recommended compliance strategies and reviewed and amended global anti-corruption policies for Bribery Act compliance. Emma also advises on drafting and amending contracts to deal with bribery risks. She has written many articles on regulatory and financial crime issues, and has spoken at several seminars, including at the British Bankers' Association, the Futures and Options Association, and the Institute

of Money Laundering Prevention Officers. She is on the editorial board of *Compliance Monitor, Financial Regulation International,* and *World Securities Law Report*. She won the 'Best Regulatory Lawyer' award at the Compliance Register Awards in 2013. She also won the 'Best Compliance Trainer' award at the Compliance Register Awards in 2006, 2011, and 2012 and the 'Best Compliance Training Programme Designer' in 2013. Emma is the editor of the firm's weekly financial regulatory e-newsletter, FReD, which won the award for 'Best Editorial Team' at the 2011 and 2012 Compliance Register Awards.

Chapter 1: Financial crime and trade finance

By Neil Chantry, global head of policy and compliance, trade and supply chain, global transaction banking at HSBC, Rosali Pretorius, partner, financial services and funds practice at Dentons, and Thierry Sénéchal, senior policy manager of the banking commission at the ICC

Background

GLOBAL TRADE relies upon accessible finance for trade transactions. Trade finance assists customers with their import and export requirements by providing import/export financing as well as country and counterparty risk mitigation. Trade finance, as a transaction banking product, is a core banking business serving the real economy. The availability of trade finance and, consequently, its ability to help companies facilitate cross-border transactions through different banks across different jurisdictions is essential to support global supply chains.

According to the Bank for International Settlements (BIS), trade finance directly supports about one-third of global trade with letters of credit (LCs) supporting about one-sixth of total trade.[1] The importance of trade finance in emerging markets is even greater.[2] Trade finance assists exporters and importers pursuing opportunities in the most challenging markets. Without the effective mitigation of risk developed by trade finance over centuries, trade would, in many cases, just not flow.

Short-term trade finance is especially important to SMEs, in particular in emerging economies. Most trade transactions require financing to be provided either by the buyer or by the seller. Several key characteristics distinguish the market for trade finance from other forms of finance. Trade finance is inherently low risk compared to many other forms of finance.[3] More than everything else, the trade finance industry is characterised by short-term maturities, with security in the underlying goods being moved in a transaction. The average tenor of a trade finance transaction is less than 180 days.[4]

Bank involvement in cross-border trading is defined by the type of transaction and the degree of security required by the transaction parties. In trade, banks typically take on several roles including:

(i) Acting as intermediaries in the exchange of documents;
(ii) Issuing performance guarantees for either party or guaranteeing payment on behalf of the buyer; or
(iii) Extending lines of credit to facilitate a transaction.

As party to a trade finance transaction, the bank reduces risk and increases liquidity for the counterparties by taking on a proportion of the risk itself. For example, LCs reduce payment risk by providing a framework under which a bank makes (or guarantees) the payment to an exporter on behalf of an importer once delivery of goods is confirmed through the presentation of the appropriate documents.

Trade finance and financial crime

Trade finance has been an area of growing attention in past years. The Financial Action Task Force (FATF), the Wolfsberg Group and the Joint Money Laundering Steering Group (JMLSG) have all drawn attention to the misuse of international trade finance by criminal organizations and terrorist financiers to move money to disguise its origins and integrate it into the legitimate economy. The complexity of transactions and the huge volume of trade flows can hide individual transactions and help criminal organizations to transfer value across borders. As financial institutions have gradually introduced increasingly effective controls to combat more traditional methods of money laundering and terrorist finance, and world trade has grown, it has perversely become more attractive to criminals to use trade finance products.

Those characteristics of trade that make it attractive to money launderers – global, and therefore subject to different standards of regulation and enforcement; often opaque, in that it can be difficult to trace the origin of the goods; and long supply chains, manufacturer, trader, consigner, consignee, notifying party, financier, shipper, insurer and freight forwarder – often also make it vulnerable to fraud.

Many countries now see sanctions – also referred to as restrictive measures – against third countries, individuals, or entities, are an essential foreign policy tool to pursue certain foreign and security policy objectives.[5] Given their key role in facilitating global trade and the international economy, financial institutions are increasingly expected to act effectively as enforcers of those sanctions policies. Regulators worldwide, but especially in the US and the UK, are placing ever higher expectations on financial institutions to manage their sanctions risk. Compliance with domestic and international sanctions regimes is now a key regulatory challenge for financial institutions, and trade presents its own specific challenges. The destination of the goods may be sanctioned, or one of the parties in a long supply chain may be sanctioned, or there may be an issue with the underlying transaction itself.

The global financial crisis of 2008–09, and resulting economic slowdown, signaled the need to review the global financial regulatory framework to reinforce the banking sector's ability to absorb economic shocks and to build a stronger, safer international financial structure. It is now widely recognised that

financial crime itself can be a threat to the stability of a country's financial sector and institutions.[6] Business organisations such as the International Chamber of Commerce (ICC) have consistently voiced strong public support for the stated goals of improving the resilience of the banking sector and combating financial crimes and money laundering.

The complexity of the global trade system makes it vulnerable to financial crime

How many containers are moving per year in Singapore?
98,000 containers moving per day in Singapore.

How many FTZs are there in the world, and in how many countries (offering special tax and economic incentives within a country)?
Over 3,000 FTZs globally active:

- 200 in the US alone, over 90 in EU countries;
- In about 135 countries; and
- Employing about 43 million people

How many transactions are logged each hour for one of the largest retail stores in the US?
1 million transactions per hour. In each minute, 168 million emails sent.

80 per cent of data is unstructured (emails, trading instructions, etc.) versus 20 per cent of structured relationship (e.g. SWIFT).

The economics of regulations

The need for a resilient financial system

Financial crime is an issue of global significance and the work being undertaken to combat abuse of the financial system by criminal and terrorist interests is of paramount importance. The banking industry supports vigorous and co-ordinated action in this regard on the part of national and international authorities in collaboration with the private sector. Financial institutions have significantly increased their efforts to prevent the financing of crime and terrorism by adding substantial compliance resources to their organisations, changing the culture of compliance within their institutions, and improving processes and controls.

Action to prevent and combat money laundering and terrorist financing thus responds not only to a moral imperative, but also to an economic need. Indeed, money laundering, the financing of terrorism, financial fraud, and other financial

crimes can have significant negative economic effects. Financial criminal activities severely undermine the integrity and stability of financial systems and may have significant negative spill over effects on the capacity of financial institutions to carry out normal business activity and provide financing, in particular to the corporate sector in the less developed and emerging markets, where they is a perceive a higher degree of financial crime risk.

As a result, the industry fully supported the need for appropriate regulations to reduce financial crime risks. For instance, recently, most business associations commented on the UK FCA thematic review[7] on the potential for unintended damage to the provision of trade finance by increased due diligence requirements when dealing with less developed or developing countries, where the infrastructure to fight financial crime is either deficient or nascent, according to FATF.

The compounding effects of regulations

At the same time, recognising the growing importance of interconnected economies, the industry finds it essential to maintain Global Value supply Chains (GVCs[8]) as a driver of growth and productivity, and to overcome constraints preventing emerging countries from benefitting from the flow of goods and services in value supply chains. In a world of increasingly fragmented value supply chains spanning across developed and emerging markets, the availability of trade finance, and the ability of banks to facilitate international trade through linkages between different banks across jurisdictions, is fundamental to ensure that international trade remains a major driver of recovery, growth, and prosperity across the globe.

Heightened compliance and risk assurance measures make it difficult for banks to maintain their existing trade relationships, and challenge their ability to support GVCs. The problem is felt more acutely by the less developed and emerging markets which are perceived to represent a higher financial crime risk. These jurisdictions are in danger of being left without access to GVCs. In particular, counterparty banks—banks that are not account-holding client banks but rather entitled to limited services for the purpose of facilitating an underlying client transaction—are faced with rising Counterparty Due Diligence (CDD) requirements and costs. Higher CDD requirements, a lack of globally consistent standards and costs constrain the ability of banks to maintain multiple counterparty relationships, particularly in developing countries. They challenge their ability to support GVCs and global growth while putting into question the viability of relationships. This has resulted in 'de-risking' – reducing in banking relationships, business lines, and activities.

Latest results from the ICC Global Trade Finance Survey[9]

The supply of trade finance continues to be constrained by many of the same issues reported in previous surveys (See Figure 1 on the next page). The three top issues that were identified as 'significant' impediments were all characteristics of issuing banks. These included 'AML/KYC requirements' (69 per cent), 'issuing bank's low credit ratings' (59 per cent), and 'previous dispute or unsatisfactory performance of issuing banks' (55 per cent).

The continued mention of these issues suggests that markets alone are not meeting demand. Moreover, according to the last edition of the ICC Global Survey on Trade finance, AML/know your customer (KYC) requirements stood out as the major inhibitor of trade finance. They are reported to have led to a decline in transactions by 68 per cent of the 298 banks participating in the ICC survey. Globally, Africa was the region that was most negatively impacted by these requirements (See Figure 2 on page 7). Among firm types, SMEs were the most negatively impacted. Onerous AML/KYC requirements led many banks to decline individual transactions. In 31 per cent of respondent banks they also resulted in the complete termination of banking relationships. Compliance with these requirements is important – banks do not want to be used for criminal purposes.

However, the compliance process is resource intensive. De-risking appears to be impacting access to trade finance, especially among SMEs and companies in developing countries. The cost of compliance for one counterparty has been cited as high as US$75,000. This cost is compounded by a lack of harmonisation between jurisdictions, a problem cited by 70 per cent of respondents. This suggests that there are some measures regulators could take to reduce the unintended consequences of compliance which contribute to trade finance gaps, lowering growth and job creation. More than a third (38.52 per cent) of respondents reported closing correspondent account relationships in 2013 due to the increasing cost and complexity of compliance (including more stringent AML and KYC).

As regulatory views may differ from examiner to examiner, regulator to regulator, and country to country, the handling of regulatory risk requires a broad compliance strategy in order to ensure its avoidance. This is why organisations such as the ICC called upon G20 Governments to take on specific recommendations, including:

- The encouragement of national supervisors to establish a framework for mutual recognition of base level CDD standards, through the FATF and BIS standards setting processes. Such a framework must assess the degree to which two countries' Risk Based Approach (RBA) country CDD standards are broadly consistent and achieve an equivalent level of risk assurance;

(The shaded sections in the Figure above appear in the same order as this key.)

Figure 1: Impediments to trade finance

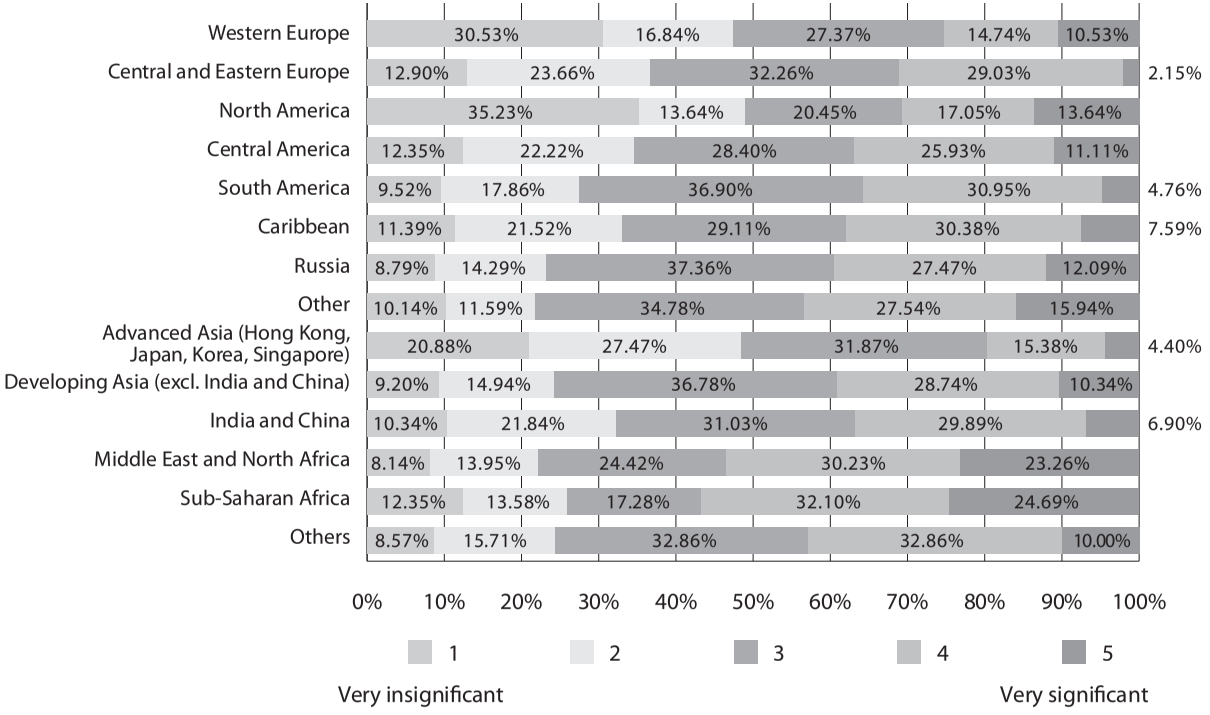

Figure 2: Regions affected by the most stringent compliance requirements

- The addition of specific guidance notes in the FATF 40 Recommendations to define the minimum financial crimes policies and procedures acceptable to the regulators so that financial institutions can set a standard approach. This would enable them to obtain acceptability from the regulators for establishing a trade-transaction-only relationship with another financial institution using the risk based approach; and
- Conducting a global study into the impact of new compliance standards on global trade flows, with special focus on SMEs and the emerging markets. Such assessment is necessary to find a balanced approach between combatting financial crime and the global development agenda.

The danger of too much de-risking

There has also been an increase in de-risking in the global financial marketplace, whereby large international correspondent banks[10] are exiting significant segments of business and further reassessing their risk appetite relative to costs associated with ensuring high standards of adherence to anti-money laundering (AML), counter-terrorism financing (CTF) and Know Your Customer (KYC) rules.[11] The no tolerance and high-penalty approach to sanctions breaches adopted by many governments has compounded the risks. With fines, such as that imposed recently on BNP Paribas running into the tens of billions of dollars it is unsurprising that banks and other financial institutions are reacting quickly to any hint that there is even the slightest possibility that a transaction might be in breach.[12] This behaviour can result in unintended consequences, among which is the risk of financial exclusion, particularly as it concerns the provision of international trade financing services in emerging markets.

The imbalance between costs of compliance and the risks of non-compliance relative to return has led to decisions by correspondent banks to de-bank respondent institutions, cease offering certain products, and cut lines of service to certain market segments. In many cases, exit is not related to actual compliance violations but rather to perceived risks and the subsequent costs of due diligence which far exceed the relationship return.[13] There are times when compliance checks on smaller customers or correspondents in emerging markets may not be cost-effective relative to scale. This can result in some deals in developing economies, particularly with SMEs, being deferred or not transacted at all. Many banks have simply pulling out of risky jurisdictions, such as Ethiopia, Indonesia, Myanmar, and even Pakistan (where only one large Western bank still maintains a significant retail banking presence[14]) altogether. With the sums of money and levels of potential reputational damage at stake, this panicked response from many financial institutions is understandable. However, it is not clear that de-risking is worth it. As *The Economist* explains:

> 'Were all of this actually preventing terrorism it might be judged a fair trade-off. Yet—and this is the second problem with this approach—it seems likely to be ineffective or even counter-productive. Terrorism is not particularly expensive, and the money needed to finance it can travel by informal routes. In 2012 guards on the border between Nigeria and Niger arrested a man linked to Boko Haram, a Nigerian terror group, with €35,000 ($47,000) in his underpants: laughable, except that the group has killed around 1,500 people this year alone. Restrictions on banks will encourage terrorists to avoid the banking system. That may hinder rather than help the fight against terrorism. A former spy complains that it has become harder to piece together intelligence on terrorist networks now that the money flows within them are entirely illicit.'

In addition, the prevalence of a zero-tolerance compliance environment has begun to overtake the risk-based approach espoused by the regulatory community, with the possibility of financial penalties, reputational damage, and individual legal culpability outweighing the business rationale for some transactions.[15] Overall, there is a growing need for a balance in combating financial crime and ensuring that the important development agenda of financial inclusion and real economy financing is not diminished. Approximately 50 per cent of adults do not have a bank account and are financially excluded in society. Whilst predominantly a developing world problem, there are also significant numbers of excluded or unbanked adults in developed regions including Europe and North America. For the unbanked, it is a challenge to gain access to banks and the services they offer. Therefore, in a world of increasingly fragmented value supply chains spanning developed and emerging markets, the availability of trade finance and the ability of banks to facilitate international trade between banks across jurisdictions is fundamental.

Trade finance: The need to facilitate financial inclusion

The provision of trade finance plays a central role in ensuring that all members of the community are economically and financially included. Restrictions on financial inclusion, in advanced and developing markets, have the potential to become a major unintended effect of increased supervisory and enforcement activity by regulators. This manifests itself in problems for banks in day-to-day operations with customers, such as restrictions on lending to businesses.

Well-intentioned rules, designed for sophisticated markets, can have powerful unintended effects, particularly when combined with other rigorous standards around new capital and liquidity rules. Harmonisation of regulations – such as those under development dealing with beneficial ownership, transparency, and a consistent approach to enforcement and sanctions –

will mitigate the cost and associated unintended consequences. This would incentivise financial service providers to embed the right behaviours to promote financial inclusion.

References

1. 'Global Survey 2014: Rethinking Trade & Finance 2014', International Chamber of Commerce, Paris.
2. The Committee on the Global Financial System, 'Trade Finance: Development and Issues', January 2014. See: www.bis.org/publ/cgfs50.pdf.
3. International Chamber of Commerce, April 2013, Global Risks: Trade Finance Report, www.iccwbo.org/News/Articles/2013/New-ICC-report-says-low-risk-trade-finance-not-to-be-feared.
4. See the 'ICC Global Risks Trade Finance Report 2013', ICC Publishing, Paris.
5. See, for example, stated European Union Common Foreign and Security Policy Objectives at http://eeas.europa.eu/cfsp/sanctions/index_en.htm.
6. See, for example, the view of the IMF at www.imf.org/external/np/exr/facts/aml.htm.
7. In 2013 the UK's FCA carried out a thematic review of financial crimes, focusing on the need to increase the levels of CDD and related due diligence that banks need to have in place to conduct the finance of international trade in a safe environment. This highlighted, amongst other issues, that on a risk-based approach, the due diligence requirements for maintaining correspondent bank relationships for trade has been significantly increased.
8. GVCs are a major driving force of globalisation. They are an inevitable outgrowth of the application of transformative information and transport technologies, combined with new business models and largely open borders. The GVC phenomenon promotes integration on multiple levels; local, regional, and international.
9. 'ICC Rethinking Trade & Finance 2014', 2014.
10. Correspondent banking is the provision of a current or other liability account, and related services, to another financial institution, including affiliates, used for the execution of third party payments and trade finance, as well as its own cash clearing, liquidity management, and short-term borrowing or investment needs in a particular currency. A correspondent bank is effectively acting as its correspondent's agent or conduit, executing and/or processing payments or other transactions for the correspondent's customers. These customers may be individuals, legal entities, or even other financial institutions.
11. From a practical standpoint, one emerging market institution interviewed by BAFT previously served as a correspondent for other emerging market institutions without a branch presence in the US from which to clear dollar transactions. However, as of 2014, the bank has closed 60 per cent of their correspondent accounts and now only conducts business with direct customers. The bank experienced a loss

of US$150m in revenue over five years as a result of exiting relationships. From a quantitative standpoint, a survey of BAFT members found that 56 per cent of respondents have decreased the number of correspondent relationships in the past three years. Over 41 per cent of respondents felt that increased compliance costs led to a reduction in transaction banking flows which ultimately impact trade and general commerce

12. See *The Economist*, 'Hitting at Terrorists, hurting business: Forcing banks to police the financial system is causing nasty side effects', 14 June 2014, see www.economist.com/news/leaders/21604172-forcing-banks-police-financial-system-causing-nasty-side-effects-hitting-terrorists.
13. For example, quantitative analysis of bank due diligence costs have found that onboarding per client can range from US$25,000–50,000, with an average yearly KYC due diligence of over 600 hours per client. This can in turn make business with smaller clients, particularly in emerging markets, less feasible.
14. See *The Economist*, 'Poor Correspondents: Big banks are cutting off customers and retreating from markets for fear of offending regulators', 14 June 2014.
15. Examination standards, for example, have in some cases deviated from the risk-based approach, with banks taking on roles beyond the normal course of a correspondent relationship and more akin to the activities of public authorities. This includes checking the ownership of both the applicant and beneficiary; validating if the ultimate buyer received the goods even though the bank acts as a confirming bank and does not have a relationship with the buyer; validating the vessel or container information; and validating the price of the goods being shipped.

Chapter 2: Integrating compliance into successful trade finance

By Sean Edwards, head of legal, Sumitomo Mitsui Banking Corporation (SMBC)

WITHOUT PROPER integration of the policies, systems, and procedures needed to deal with the financial crime and compliance risk required by their regulators, banks and other providers of trade finance run the all too real risk of either losing business or being censured by their regulators, facing fines, and worse, having their licence to operate revoked. Finding the middle ground where both risk can be avoided and profitable business can be conducted is therefore crucial. This chapter focuses on how to live and work with financial crime prevention regulation. Particular attention has been given to how marketing professionals should become involved in the compliance process, balancing limitations on their time and their optimal employment with developing a successful strategy for dealing with financial crime risks.

Categorising trade finance and developing a risk appetite

Trade finance, like any other branch of banking, is of course exposed to the risk of fraud and money laundering. Banks also face the risk of being used for terrorist financing or flouting sanctions. The challenge for trade financiers is to determine what additional financial crime risk exists in their business simply by virtue of engaging in trade finance and, once this has been determined, to provide the necessary extra resources.

Two questions need to be asked and answered before this determination can take place. First, it is necessary to categorise the different activities that trade finance departments engage in. Then the firm should assess its risk appetite for each of the activities.

Complexity of trade finance types and prioritisation

Not all trade finance is created equal, at least in the eyes of the regulators, and it is critical to ensure that resources are not allocated to the wrong area. For example, jumbo pre-export finance (PXF) transactions will not require the same amount or type of checking or verification as the purchase of rights under a confirmed deferred payment letter of credit by a non-nominated bank.

The following suggested list sets out activities in ascending order of complexity, so far as financial crime risks checks are concerned:

- Syndicated loans for trade purposes such as pre-export or pre-payment loans;
- Bilateral working capital lending to corporates and financial institutions engaged in trade finance;
- Bilateral trade-related loans to the same entities;
- Bilateral loans for the financing of specified goods or services to those entities;
- Guarantees, performance/bid bonds;
- Supply chain finance;
- Issuance of letters of credit;
- Collections;
- Re-financings of letters of credit/purchase or discounting of letters of credit, or other payment obligations such as negotiable instruments, by nominated banks or by the original holders of those instruments; and
- Purchase or discounting of letters of credit or payment obligations where the purchaser is not a nominated bank or the original holder.

This categorisation may not be comprehensive or relevant to all trade finance institutions. What is important to note is that this categorisation is not the same as the more familiar categorisation of counterparties and customers into high, medium, and low risk. What this approach attempts to tease out is, for any given risk category, first the number and transparency of the counterparties and, second, the number of documents that are likely to be available and so submitted for checking. This will be relevant to gauging what additional policies or procedures will need to be put in place to deal with the perceived additional risks arising from trade finance business.

The Financial Conduct Authority (FCA) in its thematic review of the financial crime risks in trade finance (the 'Thematic Review'[1]) has concentrated very heavily on the information and the warnings (the so called 'red flags') which only verification of documentation can provide. This, of course, is not to say that where no documentation is provided no risk exists – indeed the opposite may be the case – but, at a transactional level, monitoring and awareness of risk will most easily be judged through the transactional documentation being provided.

Determining risk appetite

Determining risk appetite is the second issue that must be tackled. At the most basic level, which customers does the bank want to deal with and what types of business will it accept from those customers? While much of the focus by regulators and industry groups has been on paper-based transactions such as letters of credit (which generate quantities of verifiable information not available with, say, open-account trading), a more fundamental and broader conception

of financial crime risk must be adopted. Factors such as reputational risk and the cost of ensuring compliance where insufficient transactional information is available should be taken into account. Such a decision will also need to take into account wider organisational and corporate governance responsibilities. Such decisions must be taken at the very highest levels of management, a point made in the Thematic Review.

Risk appetite is not, however, limited to the initial decision as to which clients to take on. It must also be applied operationally. In the words of the Thematic Review, a risk-sensitive approach must be taken and the control framework should be 'tailored to the role of the bank in a particular transaction'. The Joint Money Laundering Steering Group (JMLSG) devotes an entire chapter (Chapter 4) in Part 1 of its Guidance to Financial Institutions to this theme.[2]

This point is well-illustrated by reference to the examination of documentation in letters of credit (LCs). In LCs, a mainstay of trade finance business for many smaller banks, the standard for examination of documentation is determined by the Uniform Customs and Practice for Documentary Credits (UCP). Does the document comply on its face with the requirements of the credit as articulated in Article14 of UCP 600? The FCA considers that this philosophy has misled many banks into believing that, with the possible exception of sanctions, wider financial crime issues do not need to be considered if there is a complying document. Any such mind-set is outdated and clearly wrong. In the UK at least, the need to comply with financial crime legislation will override the rules of the UCP and excuse the examining bank from obeying Article 14. This does not mean, however, that the UCP no longer has any place in the examination of documents. It is submitted that it is only when the appropriate financial crime checks have revealed the possibility of financial crime taking place that the UCP must be ignored.

The difficulty often arises in practice when the voluminous and often highly detailed information that can now be obtained very easily as to, for example, ship movements, loading dates and so on, appears to cast doubt on a document which is in all other respects compliant. Recognising that commercial reality might result in a mismatch cannot, in and of itself, lead to the conclusion that a financial crime has occurred. A further exercise has to take place and analysis has to be carried out. An inaccurate loading date, for example, may be acceptable if it can be determined that those goods do exist and were loaded. If the information, however, shows that the goods do not in fact exist or were loaded onto a different ship, the conclusion is likely to be that a financial crime has occurred and that the transaction must be rejected notwithstanding the apparent compliance of the documents. The traditional fraud exception under English law for refusing payment under a letter of credit requires a very high level of proof that a fraud has occurred.[3] By contrast, the corresponding

level of proof under financial crime legislation is much, much lower and requires merely reasonable suspicion. (Chapter 3 covers fraud in further detail.)

Building the team and allocating the responsibilities

Infinite resources and an unlimited supply of experienced staff will never be possible. This is even truer of front-office staff who are, after all, recruited to produce profits. Does this mean that they should not concern themselves at all with financial crime risks?

The answer is unequivocally no. In the new regulatory environment the costs associated with getting it wrong must be factored into doing business. The use of front-office staff is therefore justified by the risk. The challenge is to use them intelligently, ensure they are properly supported, and optimise their involvement.

As a general rule, the use of front-office staff is optimised when they are involved in the conception and creation of arrangements to deal with financial crime risk and at the beginning of counterparty relationships. The relationship between front-office staff, non-customer facing intra-departmental resources, and separate organisational or even external resources can thereafter be mapped always with a view to encouraging efficiency both in terms of overall costs and use of time.

One way of looking at this mapping is to consider the areas explored in the Thematic Review.

The architecture of a sound and business-friendly financial crime risk strategy

Risk assessment

The involvement of marketing officers and the senior management of trade finance departments is critical at this stage because the results of this assessment will influence the complexity, cost, and scope of the systems that will ultimately need to be implemented. Importantly, the assessment will affect what trade finance products and services can be offered and to what category of customer.

This assessment must cover not only the areas of activity presently undertaken by the firm, but also potential future business. It must be as comprehensive as possible and must be endorsed by the highest level of management. Those at the very top of the firm and not just the trade finance department must be involved. (Lack of senior management awareness and involvement was an important criticism of the Thematic Review).

Building on the initial categorisation referred to above, which will act as an initial triage and give a rough indication of the intensity of both the initial effort and the ongoing maintenance of the systems, the assessment should take

account of the risk factors associated with each piece of business and customer. These factors will include:

- The jurisdiction of current or targeted counterparties or the countries where marketing will take place;
- The products to be marketed;
- The legal organisation of the counterparties and their beneficial owners;
- The business sector; and
- How products will be sold (e.g. through agents, online, in face-to face meetings etc.).

The results of this assessment can then be used to produce an overall rating or status for the type of business being undertaken, or to be undertaken, to be weighed against the firm's chosen risk appetite. This rating process can be – and to some extent must be – mechanistic (for example, by allocating weights or scores to different factors), but should always be finally evaluated against the controls which will include the value that can be attributed to marketing staff being involved in the initial assessment and, of course, as transactions begin to flow.

External data sources should be used as much as possible to produce an objectively defensible assessment. Such sources are more numerous for certain factors than others. For example, in the assessment of the risk posed by the jurisdiction, Transparency International (www.transparency.org) and the Financial Action Task Force (FATF[4]) produce information and rate countries against different indicators (such as human rights, population control, poverty etc.).

Understanding the universe of different entities involved in any line of business is critical and a current flashpoint. Customer due diligence now goes beyond knowing your immediate customer and may also require knowing your customer's customer (so-called 'KYCC'). And not just customers, but potentially correspondent banks and other intermediaries regularly used by the immediate client. In relation to letters of credit, for example, guidance has been issued by the Wolfsberg Group[5] and the JMLSG as to which parties are to be subject to due diligence, which is being reviewed in the light of the need for KYCC. Clearly the degree of due diligence required on any particular letter of credit will depend on the bank's involvement with that credit, but in view of the changed landscape it is no longer possible to stop at immediate credit risks. Amongst other things, the need to screen for breaches of sanctions (where partitioning of transactions by reference to immediate contractual counterparties does not give protection), may lead to a risk of allegations of abetting circumvention or avoidance if underlying parties are not taken into consideration. If the business being targeted is likely to involve multiple parties,

trans-shipments (etc.), all the extra costs of verifying this should be factored in up-front.

Policies and procedures

Following the risk assessment, a policy must be formulated and procedures then created to implement the policy.

Marketing, and senior trade finance staff (product and sales) must be involved in the writing of the policy. Procedures must be reviewed by them and their contribution will still be substantial but it is necessary at this point that dedicated compliance personnel should begin to weigh in more heavily.

The final policy will also either set out the risk appetite referred to above or reflect the logic stemming from that policy. It will, at a high level, explain the procedures to be implemented and allocate responsibilities and make clear the type of financial crime risks that are relevant to the business to be undertaken.

Procedures must be detailed and must be consistent with the policy in terms of scope so that, for example, banks as a matter of policy will not deal with certain kinds of products and will not need to be concerned with the risk arising from those products. Marketing and product teams must help to frame the procedures with compliance staff as they must be, for the former, realistic and achievable and, for the latter, capable of satisfying in practice regulatory requirements which ultimately have the force of law.

Due diligence

Here we are primarily concerned with customer due diligence (CDD) in the form of know your customer and anti-money laundering checks and verification. This work is often divided into up-front due diligence and on-going monitoring/ transaction due diligence.

It is very beneficial for marketing staff to be involved in up-front CDD which will involve investigation of the customer's business, often known as 'know your business' or KYB. The more comprehensive the description, the better focused the resources utilised to deal with the financial crime risks can be, and fewer then are the questions which are likely to arise when business does occur. For example, where a client has a commodity business which traditionally involves little documentation (for example, purchasing an unprocessed commodity from small local farmers), an explanation of historical practice, track record, and details of the client's final off-takers will serve to support an assessment that the customer is not running a risky business (in financial crime terms) despite a lack of voluminous documentation.

Marketing staff should also be primarily responsible for obtaining the information about the client for assessment and, indeed, for questioning that information when it is incomplete or unconvincing. This is not only because it

is easier for them to obtain such information, but also because such interaction with the client can be sensitive and is therefore best handled by those with a personal knowledge of the client. Public information should be obtained either by supporting staff within the marketing unit or dedicated compliance staff, although this ideal is not always attained in practice.

One of the greatest organisational challenges for banks in dealing with financial crime is finding the right balance and mix of staff in dealing with transactional due diligence. The focus is often too narrowly focussed around AML issues and examination of documentation.

On-going monitoring and transactional due diligence is best handled by dedicated staff with the exception of periodic reviews of the client's business. Here regulatory pressures can pull in opposite directions. On the one hand, compliance staff must be independent from the front office. On the other hand, as the Thematic Review recognises, they need to be sufficiently experienced. Squaring this circle usually requires establishment of an experienced cadre of processing staff with well-documented procedures and clear lines of referral and escalation. This is the approach recommended by the FCA in the Thematic Review which proposes, as a good operational model, a structure with two initial levels of review followed by referral to a compliance/investigations team.

Building up a good processing team is likely to be the single biggest area of expenditure when building up an effective structure. Such staff are often centred around letters of credit experts. It is critical, however, that such expertise is only a starting point in building up these teams. They must – to use the words of some commentators – be 'enlightened' and fully alive to both the nature of financial crime risks and the demands of financial crime legislation. The dangers of taking a limited face-value approach to compliance is highlighted in the Thematic Review and has been discussed above.

Such teams will look for red flags, will be aware of how far to take KYCC, and will be technically competent. Use of external suppliers is likely to be very beneficial. Particularly well-known is the International Maritime Bureau but there are a number of initiatives to establish KYC/AML databases (e.g. by SWIFT). These suppliers are likely to be expensive, however, and consequently use of these external resources must be well-judged. Automated systems to look for sanctions and other issues such as dual-use goods must be fully employed and cannot be carried out manually in a cost-efficient way.

Provided that the right staff are recruited for this role, they should also be able to apply the risk appetite or sensitivity to transactional situations mentioned above in the introduction to this chapter. If such staff are costly, the rewards of establishing the right team are correspondingly immeasurable. The cost of lost opportunities to do future business must be factored in here as much as the immediate financial cost of employment.

Governance and management information

In relation to governance, many of the concerns around organisation referred to in the Thematic Review are dealt with above. In particular, the inter-action between compliance, processing, and front-office staff has been discussed. The Thematic Review also clearly believes that audit functions have an important role to play. The growth of the paper trail, which was found deficient by the FCA in many institutions reviewed, is, in audit terms, both cause and effect. If proper structures are put in place there is nothing to fear and much to embrace in audit reviews especially in the early days of operation.

The involvement of senior management is also emphasised. Senior management can assist by setting the tone, but they must also be part of the chain of escalation. Corporately and operationally, this will only work if lower levels have fully investigated all the issues and have attempted to solve them. Routine referral to senior management is, in most cases, not desirable as it will delay resolution and dull the determination of more junior staff.

Production and delivery of management information must, however, be routine and regular. This can be either direct to the senior management or to appropriate committees. Although production of this information is best left to processing and compliance staff, any questioning by senior management should also involve and be directed to front-office staff as it may touch on issues of wider concern.

Training and awareness

Training flows from and to front-office staff. It will flow to them in the form of awareness of and sensitisation to financial crime risks. This may be delivered by compliance staff or external providers. It will, however, also flow from marketing officers to compliance and processing staff as a part of an iterative process to produce targeted training that is relevant for the bank and its particular business. A complaint often made is that back and middle office functions do not understand the very specific nature of much of trade finance. Realistically, producing good quality training must involve marketing staff at least during initial development.

Marketing staff are particularly invaluable when producing training material based on case studies. The FCA has said this is a useful form of training.

Conclusion

An intelligent and constructive approach is required to the management of financial crime risks in trade finance. The complex nature of trade finance has meant that it has appeared, to many regulators and compliance personnel, to be an area open to abuse. This is not always a well-founded conclusion and it is within the gift of the trade finance community to remedy this misapprehension.

This chapter has shown that with proper integration of marketing staff a solution is available. In other words, when those responsible for communicating the bank's trade finance products and services to potential customers have a thorough grounding in financial crime risk prevention, the bank will manage customer expectations appropriately. This will require more investment in regulatory and compliance issues than has hitherto been the case by these areas, but it must be accepted that, without such involvement, the wheels of trade finance will grind ever more slowly.

References

1. See 'TR13/3 - Banks' control of financial crime risks in trade finance', July 2013, at: www.fca.org.uk/news/tr13–03-banks-control-of-financial-crime-risks-in-trade-finance. See also: www.tfreview.com/news/legal-regulatory/fca-financial-crime-risks-final-guidance-softens-kyc-position.
2. 'Chapter 4: Risk-based approach', in P*revention of money laundering/combating terrorist financing*, Joint Money Laundering Steering Group, 2011. See: www.jmlsg.org.uk/download/7324.
3. See *United Trading Corp SA v Allied Arab Bank Ltd* [1985] 2 Lloyd's Rep. 554; Times, July 23, 1984.
4. An intergovernmental body set for 'the development and promotion of national and international policies to combat money laundering and terrorist financing'. The FATF comprises 34 member jurisdictions and two regional organisations representing most major financial centres in all parts of the globe. See www.fatf-gafi.org for further information.
5. An association of 11 global banks whose aims are to develop industry standards and related products for KYC, AML, and counter-terrorist financing policies. See www.wolfsberg-principles.com for further information.

Chapter 3: Fraud in trade finance

Clarissa Dann, editor, Trade & Forfaiting Review

THE SPECTRE of fraud lurks in most areas of domestic and international commerce, and trade finance is no exception. As demonstrated by China's Qingdao Port scandal[1] where multiple loans were secured against the same collateral, and the pre-financing scam highlighted by ICC where false shipping documents were presented to trigger payment under a letter of credit (LC),[2] no cross-border trade transaction is immune from this particularly insidious form of financial crime.

Fraud not only damages businesses and banks, but also entire economies. For example, in May 2014, a study from Global Financial Integrity revealed that the over and under-invoicing of trade transactions facilitated at least US$60.8bn in illicit financial flows into or out of five specific African countries between 2002 and 2011.[3]

This chapter reviews the specific risks and examples of fraud involving the use of trade and commodity finance instruments, and it suggests some practical approaches to fraud prevention.

UNCTAD commodities finance fraud 'primer'

Although written more than ten years ago, every commodity finance professional would do well to review Lamon Rutten's 'primer' on new techniques used by financial fraudsters in the commodities markets.[4] Now manager of policies, markets, and ICT at the Technical Centre for Agricultural and Rural Cooperation (CTA), at the time of writing in March 2003 Rutten was an economist at the UNCTAD secretariat. His introduction sets out a telling perspective on what makes an organisation vulnerable to fraud in the first place.

> 'If an organisation is badly managed, the potential for fraud and abuse increases. Proper government regulations can prompt organisations to put basic controls in place, and can force them, to some extent, to be transparent about their dealings, but not even a perfect regulatory framework can replace proper company-level control systems for the use of financial instruments. A lack of checks and balances, unclear reporting lines and an unclear division of responsibilities all contribute to an environment in which staff may feel that they can commit fraud and get away with it.'

Rutten continues:

> 'The remedies for this are well known, although they are not necessarily applied even in large organisations. The division of responsibilities needs to be spelt out and measures [need to be] taken to ensure that responsibilities are met. Reports on transactions from outside parties (e.g. brokers, collateral managers) should not go to the person that initiated the transaction. Multiple checks and balances need to be built into the system – for example, to separate the responsibility for entering into financial transactions from cash flow management responsibilities, and the two individuals or departments controlled by yet another person/department – and all should report to a specific member of senior management.'

Rutten emphasises that a manager should keep an eye out for unusual behaviour: 'Managers should be aware of possible signs of trouble – for example, traders who regularly come in over the weekend, and who may use the time to tamper with computer systems or records, or who do not take any holidays for fear that their temporary replacement could discover fraud.'

The ICC Commercial Crime Services

Based in London, the ICC Commercial Crime Services (CCS) is the anti-crime arm of the International Chamber of Commerce. The International Maritime Bureau (IMB) is one of its specialised divisions, with the main task of protecting the integrity of international trade by seeking out fraud and malpractice. The information gathered from sources and during investigations is provided to members in the form of timely advice via a number of different communication routes without identifying the sources. The IMB lists the threats and explains how members can reduce their vulnerability to them. In particular, the IMB provides an authentication service for trade finance documentation. It also investigates and reports on a number of other topics, notably documentary credit fraud, charter party fraud, cargo theft, ship deviation, and ship finance fraud.

The IMB verifies 2000 trade transactions and bills of lading every week. While this is a small proportion of the global volumes it gives the IMB enough insight to spot patterns and identify what documents might be forged or disguised to bypass sanctions screening. The IMB also conducts post-fraud investigations and provides expert evidence. For further reference, Mukandan summarises the IMB's activities in a helpful video which can be viewed online at www.youtube.com/watch?v=5wy58e8jf1U.

The CCS director, Pottengal Mukundan, is a popular speaker at trade finance and compliance conferences and specialises in the investigation, detection, and prevention of onshore and offshore commercial and maritime

crime. He makes the point that the Uniform Customs and Practice for Documentary Credits (now UCP 600) discourages banks from assuming responsibility outside the compliance of the documents presented. 'Banks take the view [that] they are merely financing the trade transaction. They do not assume responsibility for the existence or quality of the commodities traded. The system is based on documents. Documents can be forged', he once told the editor of *TFR*.

The letter of credit and the fraud exception rule

This section summarises a talk given by trade finance lawyer Geoff Wynne at the International Trade and Forfaiting Association conference in 2011 (at the time of the conference, Wynne was a partner at Dentons, but is now at Sullivan & Worcester UK). This section sets out a reminder of the principles of a letter of credit (LC) and where it is possible for a bank to refuse to pay out when presented with an LC if there is sufficient evidence of fraud. As will be seen, the fraud argument is sometimes deployed as an excuse not to pay up and it falls to the courts to decide whether fraud was present or not.

Transaction independence – When is a letter of credit that is 'synthetic' still a letter of credit?

When the Abu Dhabi Islamic Bank argued that the 'synthetic' structuring of the LC it had confirmed to Fortis Bank meant it could legitimately refuse payment, this tested the resilience of the LC with some important implications for structured finance arrangements.

The case of *Fortis Bank (Nederland) NV v Abu Dhabi Islamic Bank* (heard by the Supreme Court in New York in August 2010), highlighted the independence of the LC from the underlying trade transaction, and how the use of fraud as an argument not to pay does not really wash when all parties were aware of the structure of the transaction. The box out below summarises the facts of the case.

This was a synthetic transaction in that it was not fully related to an underlying trade transaction, but was used to generate finance for the beneficiary. However, the judge gave very short shrift to ADIB's arguments that its synthetic nature meant it was fraudulent.

Fortis Bank (Nederland) NV v Abu Dhabi Islamic Bank

- A deferred payment LC was issued by Awal Bank (Bahrain) and confirmed by the Abu Dhabi Islamic Bank (ADIB) in June 2008 on behalf of Bunge (a large European commodities trader for US$40m to facilitate the sale of Brazilian soybeans and maize).
- This was a 'synthetic' transaction as it was not really related to an underlying trade transaction.
- ADIB confirmed its reimbursement obligation to Fortis.
- ADIB then did not wish to pay. Awal, the issuing bank, had gotten into difficulties and ADIB knew it would not receive payment from them. ADIB alleged fraud.
- Fortis sued and won. The judge held that all parties were aware of the transaction structure and the documents were in order.

The full case report, including the judgment, can be viewed at http://law.justia.com/cases/new-york/other-courts/2010/2010–52415.html.

Letters of credit – A reminder

What makes LCs so useful is that they are an irrevocable payment undertaking given by (usually) a bank, and payment is made against documents presented in accordance with UCP 600, the current Uniform Customs and Practice for documentary credit rules. When this happens, both the confirming and issuing bank are liable for the payments. It is important to remember that an LC is a transaction in documents. Documentary letters of credit are usually payment instruments, but they can be used as financing instruments – and many parties use these for financing in the context of deferred payment undertakings and the refinancing of LCs. This is not unusual.

UCP 600 is very specific about the roles, duties, obligations, and rights of the issuing bank, the advising bank if there is one, the confirming bank, and the nominated bank (which may be the negotiating bank). The *dramatis personae* in *Fortis* are really the issuing, confirming, and nominated bank. UCP 600 requires documents to be presented and examined within agreed standards and timescales. Letters of credit can be available by sight payment, deferred payment, acceptance, and negotiation. This case was about deferred payment LCs and, to a certain extent, the other parties are outside of UCP 600. The applicant and beneficiary are mentioned in the UCP 600, but their rights and obligations are outside these and are often documented separately.

Once the beneficiary has its money and the bank has made its paid, what follows is an interbank transaction. The nominated bank/confirming bank makes payment and the confirming bank looks to the issuing bank. In the normal course of events, if the bank has given value on an LC it will always be paid by the

confirming bank or issuing bank under that LC. The one big exception is fraud, which was why ADIB chose that argument to try to avoid payment on that basis.

Fraud unravels all

We have established that the LC is independent from the underlying transaction and that, if the right documents are presented, the confirming bank and anyone else who has accepted liability has to pay. In other words, what makes LCs sacrosanct is certainty of payment.

However, the fraud exception operates, for example, where the seller/beneficiary, for the purpose of drawing on the LC fraudulently presents to the confirming bank documents that contain – expressly or by implication – material representations of fact that they know are untrue or are otherwise fraudulent on their face. Where this is the case and the bank is aware of the fraud, then it is entitled to refuse payment if it finds out before the payment – and to recover the money as paid under the mistake if it finds out afterwards.

That was and is the basic rule and, despite many attempts to look at widening the fraud exception rules, there have been few successes. One example was *Solo Industries v Canara Bank* (2001), where a fraudulent misrepresentation to induce an LC was a defence of non-payment.[5]

In answer to the question of whether or not a buyer can refuse to reimburse the bank for paying the seller when fraudulent documents were present, the following needs to be noted:

- The fraud exception only takes effect where a beneficiary's fraud is evident and the bank is aware of this before payment;
- A buyer will only be entitled to refuse to reimburse the bank where a beneficiary has presented fraudulent documents and the bank has failed to take reasonable care in inspecting the documents to verify compliance with the terms of the LC;
- UCP 600 has provided for a different standard of inspection from UCP 500. Article 14(a) (replacing UCP 500 13(a)) no longer stipulates that the examination be made with reasonable care – 'a ... bank must examine a presentation to determine, on the basis of the documents alone, whether or not the documents appear on their face to constitute a Complying Presentation'; and
- The net effect of all the above is that provided a bank can: (a) satisfy itself that the documents are a Complying Presentation according to UCP 600; and (b) has neither irrefutable evidence of a beneficiary's fraud nor clear evidence of such fraud which the beneficiary has failed to refute, then that bank should pay the beneficiary under the letter of credit and be entitled to be reimbursed by the buyer for doing so.

Implications of *Fortis*

There are a number of 'synthetic schemes' in existence – with many of them having been called 'Bunge schemes', as Bunge had promoted them. These were devices used between two related companies within the same group that can produce financing opportunities for banks in emerging markets. They rely on LC and UCP 600 treatment of LCs and the concept of compliant document presentation and deferred payment undertakings.

The *Fortis* case was unconventional in that copies were requested instead of original bills of lading. There is actually nothing wrong in this and goods do not actually have to move to be a trade transaction – warehouse financing is a good example of this principle.

One bank offering a refinancing facility for an LC to another is, in theory, a continuation of a trade transaction – it is valid but perhaps more akin to a working capital facility. The important thing is to ensure that a real transaction is in place. English courts analyse the documents and look at what has been structured on the transaction, and make decisions on that basis rather than seeking to rewrite the deal. In *Fortis*, that was what the New York court did as well.

The 'when trade got paid' successes for trade payment following the Kazakhstan banking crisis was more about the priority given to short-term indebtedness where there was not enough money to pay all the creditors – the validity of the original transactions was never in question.[6]

Learning points from *Fortis*

Fortis was an important case because it highlighted the arguments about what the underlying transaction is really about, and its relationship with the original trade. It also demonstrated that these more unusual transaction structures can be risky if not properly documented in line with UCP 600, although they are workable in certain circumstances. It is vital that it can be demonstrated that all parties know what the transaction is and have complete and transparent information – so that there can be no defence of fraud.

Last but not least, structured transactions of this nature are dynamic and need to support the will to do deals and structure them so that everyone can make a profit – which means having certainty and getting paid.

Warehouse fraud

On 11 September 2011, Qingdao Port in China's Shandong region confirmed that the metals financing fraud had involved around 400,000 tonnes of base metals. This was made up of around 300,000 tonnes of alumina, 80,000 tonnes of aluminium ingots, and 20,000 tonnes of copper. The same

consignments of metals had been pledged multiple times by borrowers to raise trade finance loans.

The investigation prompted lawsuits from trading firms, warehouses, and banks around the world, including HSBC and Standard Chartered. The scandal was a wake-up call to the industry. For the banks, the suspected fraud is a warning shot.

Vivienne Lloyd, base metals analyst at Macquarie Securities, told the *Wall Street Journal* in September 2014 that banks have tightened up on issuing letters of credit, which has made it harder for importers to get hold of metal. She said: 'It has definitely changed the conversation around risk in metals financing'.[7]

This is just one example of how vulnerable banks can be when loans are secured on commodities. Accidents do happen. One banker told *TFR* how a particular consignment of tobacco he was financing literally self-combusted in the warehouse because of errors in storage and temperature – and insurance protection is one means of mitigating that risk. But if fraud is involved and the goods never existed in the first place, the insurer is unlikely to pay the claim.

Warehouse woes – Supply chains can become vulnerable to fraud

Global economic activity looks set to pick up. However, with increased trading activity comes more risk, such as the potential for international fraud relating to goods in storage. Warehousing provides a vital function in the international trade of commodities, but it also provides the potential for serious losses when things go wrong. Several high-profile cases in recent years illustrate the legal difficulties, risks, and complexities involved in fraud cases.

Singapore Tin Industries

Perhaps one of the best-known cases of supply chain fraud relates to the collapse of Singapore Tin Industries (STI). The case involved a claim by ABN AMRO, a category II member of the London Metal Exchange, against CWT Commodities, under a collateral management agreement (CMA).[8] Under the agreement, CWT was obliged to issue warehouse receipts and certificates of quality for tin that STI was using as security for trade finance as provided by ABN AMRO. To store the metal, CWT leased a warehouse at STI's premises.

CWT issued certificates of quality and warehouse receipts in relation to tin ingots, concentrates, slag, and also seven batches of tin dross. The bank advanced over US$22m to STI, of which at least US$10m was not repaid. It transpired that STI had been acting fraudulently by, as the judge put it, 'round-tripping' the tin dross inventory. The seven batches of tin dross were reportedly purchased from and sold on to third parties in transactions financed by the bank. In reality, no actual sales of the tin dross were made by STI and it was left in the warehouse and mixed with additional tin dross produced by

STI to provide security for additional rounds of financing by the bank. As the Singapore judge commented: 'The reality was that the bank was advancing money on the security of tin dross produced entirely by STI and left to accumulate in the warehouse.'

Stone & Rolls

Another notable example of warehouse fraud was the losses incurred by Komerční Banka, a Czech bank, through finance provided to Stone & Rolls, a Geneva-based trading company. In that case, estimated losses of around US$250m were incurred under 30 LCs issued in relation to large quantities of Russian and Ukrainian agricultural products sold by Stone & Rolls.

Komerční's problem was that there were no genuine sales of produce stored in Russian warehouses; the invoices and warrant lists presented were sham, and Stone & Rolls was found to have participated in a dishonest scheme designed to defraud the Czech bank.

A United Nations working paper on warehousing issues has also highlighted similar problems in other cases.[9] In one example, several Hungarian banks incurred losses where they had provided finance against warehouse receipts which, it was eventually discovered, had been issued by private rather than public warehouses. In another case, US banks provided finance for imports of commodities into Russia, but faced losses when it was discovered that the warehouse receipts provided for the goods were fake.

Risk factors

Although supply chain fraud cases are usually complex and generally turn on their own distinct sets of facts, there are some common risk factors that can be identified as key areas of concern:

- Accurate monitoring of warehouse goods and the method of storage: An obvious but all too common issue is determining whether the goods ever made it into the warehouse in the first place. Fraud on the part of the warehouseman or other party issuing warehouse receipts can mean that the goods simply never arrived – a problem that can have a significant impact on insurance claims. Other problems can involve theft, forgery, or false endorsement of the receipt.
- If the goods made it to the warehouse, are they still there? Poor warehouse security and management can result in theft, misappropriation, or misallocation.
- Both storage methods and the clear segregation of goods within the warehouse can be significant: Given that the insolvency of the warehouse can be a complicating factor, a major aspect in ensuing litigation is often

the resolution of competing proprietary claims to goods that are recovered. Inability to identify consignments is a significant complicating factor in such disputes.

- Potential conflicts of interest can also lead to problems where a party both owns a warehouse and uses it to store its own goods.

Because these issues are so varied, when things go wrong they inevitably lead to legal proceedings that tend to be complex. Before taking a look at some of the practical steps that can be taken to minimise risk, it is worth considering the common legal difficulties.

When goods go missing, parties inevitably tend to look to their insurance cover for recourse. Unfortunately, insurance claims in relation to supply chain losses can raise some tricky legal issues and false comfort. For example, even though an insurance policy governed by English law may provide cover for theft, where the loss occurs in another country it is quite possible that the meaning of theft may not be limited to the English technical definition.

While in England it may be sufficient to support a claim for theft by establishing a *prima facie* case of intention to steal together with a dishonest appropriation, in other jurisdictions (for example Russia) it may be necessary to show that there has actually been a prosecution or conviction for theft in relation to the incident in order for it to constitute theft under the policy.

A more fundamental problem can occur when it transpires that goods were never actually delivered to the warehouse, for example where fraudulent warehouse receipts have been issued. In such cases it can mean that risk in relation to those goods is not covered under the insurance policy, as the goods never existed, with the result that no recovery can be made.

Although it is sometimes assumed by holders of entitlement that their insurance policy (or warehouse policies) will cover them in the event of fraud, if it turns out the goods never existed, the chances are they will not be protected.[10]

In cases of insolvency, there is often extensive litigation to determine property rights in the face of competing claims by creditors. Unlike the strength and clarity of the entitlement to metal embodied by a London Metal Exchange (LME) warrant, entitlement to goods/materials held by other warehouses can be far more complex.

Invariably in cases involving fraud there is insufficient property recovered to meet the competing claims. Again, the jurisdiction in which the property is located becomes a key factor given that the relevant law governing property rights is generally the place where the asset is held (the lex situs). Title disputes relating to unsegregated products can be particularly difficult, whatever the jurisdiction. The result is that although parties may have taken great care in choosing the law that governs their contractual relationships, they may find

this to be irrelevant when determining whether they are able to defend their proprietary rights against competing creditors.

Practical steps

From these practical problems and litigation traps there are a number of lessons that can be learned to minimise the risk of warehouse fraud:

1. Warehouse arrangements: Inevitably, initial attention should focus on the warehouse arrangements themselves. Care should be taken to establish the legal and beneficial ownership of the warehouse, as well as the suitability of the facilities. Investigation of previous losses from the facility due to theft or fraud can be informative, as well as the insurance arrangements and claims history. Where a CMA is used, care is required to ensure that the control and supervision provisions relating to the goods are suitably robust and that the task is entrusted to an independent, approved collateral manager.
2. Understand which country's law applies: Given the importance of the lex situs both for insurance and insolvency claims, it is advisable at an early stage to gain a clear understanding of the applicable law of the country in which the warehouse is located. Security or proprietary interests in the goods should be protected under local law wherever possible, and this should be reflected, where necessary, in the storage arrangements or CMA.
3. Insurance: Finally, great care should be taken concerning insurance arrangements. The terms of cover require careful scrutiny, with particular regard to whether all the anticipated risks are covered, including the effect of local law upon interpretation of the policy. As we have seen, fraud can pose particular challenges in this context and specific fidelity cover for misappropriation or fraud should be obtained where appropriate.

Tread carefully

Although warehouse fraud, in relation to metals at least, is relatively rare, when problems do arise they are invariably complex and expensive. The difficulties in minimising exposure to such risks are, to a great extent, practical in terms of identifying and protecting against risky procedures. However, significant legal issues can also arise to trap the unwary and lead to exposure and losses that may be considerably greater than anticipated. Care taken to address issues of applicable law, title, and insurance at an early stage can do much to provide protection against potential fraud.

References

1. See Bernard Goyder's summary of the scandal, 'Phantom metal - the Qingdao port scandal', *TFR*, September 2014, at: www.tfreview.com/node/10904.
2. See the pre-financing scam involving false shipping documentation highlighted

by the ICC International Maritime Bureau in August 2012 at: www.tfreview.com/node/8108.

3. Baker, R., Clough, C., Kar, D., LeBlanc, B., and Simmons, J., 'Hiding in Plain Sight: Trade Misinvoicing and the Impact of Revenue Loss in Ghana, Kenya, Mozambique, Tanzania, and Uganda: 2002–2011', *Global Finance Integrity*, May 2014. See: www.gfintegrity.org/report/report-trade-misinvoicing-in-ghana-kenya-mozambique-tanzania-and-uganda/.
4. Rutten, L., 'A primer on new techniques used by the sophisticated financial fraudster, with special reference to commodity market instruments' (report prepared by the UNCTAD secretariat), March 2003. See: http://unctad.org/en/Docs/ditccom39_en.pdf.
5. *Solo Industries UK Ltd v Canara Bank* [2001] EWCA Civ 1059. The full judgment can be viewed at www.simic.net.cn/upload/2008–07/20080702161112103.pdf.
6. For a feature on how trade did 'get paid' during the Kazakhstan banking crisis, see 'IFA world: When trade does get paid...', *TFR*, February 2011, at: www.tfreview.com/node/6405.
7. Curran, E. and Inman. D., 'Missing Qingdao Copper Spawns Web of Lawsuits', *The Wall Street Journal*, September 2014. See: http://online.wsj.com/articles/missing-qingdao-copper-spawns-web-of-lawsuits-1411409796.
8. See Day-Robinson, D. and Kenny, M., 'In safe hands, the practicalities of collateral management explained', *TFR*, March 2012, at: www.tfreview.com/node/7542.
9. See: www.ruralfinance.org/fileadmin/templates/rflc/documents/Review_of_Warehouse_pdf.pdf.
10. See Sullivan, M., 'Will insurance pay? Not always under English law', *TFR*, January 2013, at: www.tfreview.com/node/8519.

Chapter 4: Money laundering

By Robert Parson, partner, and Imogen Holmgren, trainee, Reed Smith LLP

MONEY LAUNDERING is defined by the Financial Action Task Force (FATF) as 'the processing of… criminal proceeds to disguise their illegal origin' in order to 'legitimise' the gains of criminal property.[1] Based on the estimates of the International Monetary Fund (IMF) and the United Nations Office on Drugs and Crime, it is estimated that 2–5 per cent of the global GDP is laundered every year by criminal organisations.[2] A high proportion of that figure involves cross-border transactions. The suppression of money laundering activities which make use of trade payment channels is a goal which all involved – traders, banks, regulators, and law enforcement agencies – are keen to achieve. The involvement of organised crime in trade payments has led to additional regulatory and other scrutiny in an already heavily regulated sector. There is some evidence that the introduction of the measures necessary to combat money laundering has, and will continue to, apply a brake to trade growth and increase costs.

Money laundering offences and obligations relevant to the trade finance sector

The anti-money laundering regime applicable to financial institutions in the UK is extensive and covered by more than one source – those being legislation, regulation, rules, and guidelines. The key elements of the applicable framework for countering money laundering that are currently in place in the UK are the following:

- The Proceeds of Crime Act 2002 (as amended) (POCA);
- The Money Laundering Regulations 2007;
- HM Treasury Sanctions Notices and News Releases; and
- The FCA Handbook.

Money laundering related offences relevant to the trade finance sector

Several offences related to money laundering exist, and the groups of offences that concern players in the trade finance sector (i.e. financial institutions and financial organisations – and their customers) are the following[3]:

- Performing any act with knowledge or suspicion that it will assist in concealing, or entering into arrangements for the acquisition, use, and/or possession of criminal property;
- Failing to report as soon as practicable any knowledge, suspicion or, where there are reasonable grounds for knowing or suspecting, that another person is engaged in money laundering; and
- Tipping off a person suspected of money laundering: (i) that disclosure has been made to a nominated officer (e.g. a Money Laundering Reporting Officer generally referred to as the MLRO) or law enforcement authorities; or (ii) that an investigation into allegations of money laundering is contemplated or is currently taking place, where this is prejudicing or likely to prejudice an investigation or proposed investigation.

POCA provides that a court is to take into account whether the alleged offender followed any relevant guidance issued by a supervisory authority or other regulatory body and approved by HM Treasury. The guidance that has been approved is that of the Joint Money Laundering Steering Group (JMLSG).

The Money Laundering Regulations 2007 also place a general obligation on players in the trade finance sector (and generally on all those that are deemed at risk of being involved with money laundering) to establish and maintain adequate and appropriate risk-based policies and procedures to prevent money laundering, notwithstanding whether or not money laundering takes place. The Regulations provide that the policies and procedures must cover customer due diligence, reporting, record-keeping, internal control, risk assessment and management, compliance management, and communication.

Under the Financial Services and Markets Act 2000 (FSMA), the Financial Conduct Authority (FCA) may initiate proceedings for offences under prescribed regulations relating to money laundering where the failure to comply with them constitutes an offence.

With respect to FCA-regulated firms, the Senior Management Arrangements, Systems and Controls requires that such firms have 'effective systems and controls for countering the risk that a firm might be used to further financial crime, and specific provisions regarding money laundering risks'.[4] Furthermore, the FCA Handbook of rules and guidance provides for standards and practices that are applicable to all FCA-regulated firms and to all 'approved persons'. In particular, the FCA Handbook requires the implementation of appropriate systems and controls over the management of money laundering risk.

Other international initiatives

Other international initiatives that may impact on trade finance players are the offences under the US Patriot Act and further international guidance such as that provided by The Wolfsberg Group,[5] and the FATF guidance on

anti-money laundering on an international scale. The Wolfsberg Group has issued numerous guidelines on money laundering issues arising in the course of correspondent bank to bank business in which general and sector specific principles are provided.[6] FATF issues the International Standards on Combating Money Laundering and the Financing of Terrorism and Proliferation which has as its goal the provision of minimum international standards for action to ensure that the efforts to prevent money laundering are applied consistently at an international level.

The proposed 4th Anti-Money Laundering Directive

In March 2014, the European Parliament approved the draft of the 4th Anti-Money Laundering Directive in which a key feature is the obligation on each member state to implement and maintain publicly available ultimate beneficial ownership registers for both corporate entities and trusts. Given the widespread involvement of offshore trading entities in 'tax efficient' jurisdictions and the frequent creation and use of special purpose offshore corporate vehicles in complex trade and commodity structured financings, the imposition of such a regime could have a substantial impact upon the time and cost of compliance. This may require market participants to rethink traditional approaches to financing.

There is some uncertainty as to the timetable for the formal issuance of this directive. The draft directive first needs to be approved by the European Council prior to implementation by each member state.

Money laundering in trade finance

Description of the sector and the methods of money laundering in the trade finance world

In accordance with the Wolfsberg Group Trade Finance Principles,[7] trade finance can 'in its broadest interpretation, be described as being the finance by financial institutions of the movement of goods and services between two points, both within a country's boundaries as well as cross border'. So the vast majority of financially settled international transactions fall within that broad definition.

An attractive market for money launderers

Trade is attractive to money launderers for the following reasons:

- Size: Global trade is over US$35 trillion per year.
- Numbers: Tens of thousands of transactions take place every day, in amounts varying in value from a few hundred dollars to over USD100 million for a crude oil transaction.

- Geography: Global trade really is global with goods and service transactions involving literally every country in the world.
- Mode: Transactions take place by road, rail, air and water and all combinations of these transport methods.
- Abundance: Many banks offer trade finance solutions to their clients and are keen to expand their business, making trade finance abundantly available.
- Opaque: Due to globalisation of production, assembly, as well as distribution, it is becoming virtually impossible to assess the actual origin and end-use of products (for example, German cars made in China exported to Australia, or French handbags produced in Thailand sold in the USA.).
- Long supply chain: manufacturer, trader, consigner, consignee, notifying party, financier, shipper, insurer and freight forwarder.
- Regulations: Not every jurisdiction regulates trade transactions, within certain jurisdictions there are Free Trade Zones.
- Coordination: Customs and regulatory bodies are not joined-up internationally.
- Lack of control: an estimated 80 per cent of payments for trade transactions takes place on an open account basis, making it virtually impossible to check if the transaction is real.

Based on a report entitled 'Illicit Financial Flows from Developing Countries: 2002–2011' by the organisation Global Financial Integrity,[8] it is estimated that 80 per cent of illicit funds from developing countries are laundered through trade. Another report, published by PwC in September 2014 and entitled 'Goods gone bad: Addressing money-laundering risk in the trade finance system' ('Goods gone bad'), estimates that the amount of illicit funds from developing countries laundered through trade increased from 2002 to 2011 from US$200bn to US$600bn.[9] This increase demonstrates that money launderers have become more interested in laundering money through trade over the last couple of decades. This is not only due to the nature of the market, but also the lack of enforceable harmonised global monitoring structures and procedures, and to the increase of efforts to target alternate means of laundering dirty money in other markets.

A global market

Today's market operates on an international scale with enormous volumes of trades carried out each year (in 2013, the total aggregate value of world merchandise export and commercial services exports amounts to over

US$23tn – of which over US$18tn is merchandise – based on the World Trade Organisation's statistics[10]). The scale of this market makes it extremely difficult for enforcement entities and for financial institutions to determine which 'needle in the haystack' is illicit, especially when the money launderers choose their methods with care. As an example, if money launderers are only slightly 'over-invoicing' products from say US$15 to US$16 per tonne/metic ton (MT) (please see below for an explanation of over invoicing), this may be difficult for financiers, regulators or law enforcement agencies to distinguish from innocent fluctuations in market prices unless these are set against a precise accountable industry benchmark. This becomes even more difficult in volatile markets such as commodity trading.

Market trends: The increase in 'open account' transactions

Based on the figures of the 2014 ICC Global Trade and Finance Survey,[11] the volume of SWIFT trades (i.e. collections, guarantees, letters of credit) reduced by 0.65 per cent as a proportion of the total amount of trade flows meaning that trading on 'open account' terms increased – a sign of increased confidence in the market. Trading on 'open account' terms means the buyer and seller agree on the terms of the provision of the goods and the payment (or the netting of the payment) is made directly through the banking system without the provision of any credit from financial institutions. It is generally acknowledged in the market that between 70–80 per cent of global trade flows are now made on 'open account' terms. This means that it is more difficult for financial institutions to fully discern the nature of the commercial transactions and they may only be in a position to monitor transactions based on the standard anti-money laundering and sanctions screening on clean payments (and netting of payments).

Complex transactions

For dealings that are not on 'open account' terms – i.e. when credit is provided by financial institutions – trade finance transactions can often be complex with many different parties (normally more than one financial institution is involved) located in different countries, acting in different capacities, with diverse interests. Trade finance is fragmented in nature.

In this respect, trade finance operations can take many forms. They can involve any of the following:

- Transmission of funds with presentation of certain documents (e.g. shipping documents) or provided on a conditional basis (e.g. where a specific event has to occur);
- Granting of undertakings where payment will take place in the event of default (e.g. bonds, guarantees, indemnities, and standby letters of credit); and

- Financing complex structures where the financing is the main focus and the provision of trade finance instruments is only considered as secondary (e.g. securitisations, involving special purpose vehicles).

A market with a traditional approach

The trade finance industry is considered as a traditional market compared to other financial sectors that operate and rely mainly on IT platforms, though there has been a steady increase in volume of trade across supply chain finance platforms in recent years. The trade finance industry relies on the trust developed over the generations in its paper instruments and documentation process (e.g. letters of credit (LCs) and shipping documents such as bills of lading). With a wide variety of trade finance instruments, as mentioned above, this traditional approach to trading involves a great many paper instruments. For anti-money laundering purposes these must therefore be managed in large part manually to determine any risk. Automated processing of LCs and other payments is now the norm across a large proportion of international trade transactions but, particularly in developing countries, many areas of international trade remain paper bound. The processing of LCs is therefore a considerable operational burden for financial institutions in terms of cost and time, and from an operational risk perspective it is also subject to human error – evidenced by the continuing high number of discrepancies which are not caught at the first inspection by a bank of documents presented for payment. Human error can be limited by the use of the red flags system by staff. (See below for more detail on the red flags system.)

Lack of harmonisation

The international trade market is a global market where goods are exported and imported to different countries around the world. This characteristic means that the actors in this market and in trade finance transactions must abide by the anti-money laundering laws, regulations, and rules applicable in the different jurisdictions that they encounter. As trade finance transactions are also document heavy, in most instances national law will apply to these instruments (e.g. national law will, in most cases, be applicable to the enforcement of a bill of exchange). This specificity renders the monitoring of financial institutions and the investigations conducted by governmental bodies into their transactions more difficult.

Discrepancies and deviation from standard practice are routinely waived expressly to prevent the trade finance system becoming clogged with minor disputes as to form and content of documents. Even where payments are made through bank issued payment instruments, there is a limit to the degree of worthwhile scrutiny which financial institutions can bring to bear on individual

payments in 'real time' – where the performance by a contract party and its banker of payment obligations is time critical. Even where time is available, the nature of the payment obligation means that the paying bank cannot see precisely how the sum paid is commercially justified. By way of example, international supply contracts awarded by competitive tender will frequently require the provision of a local law governed performance bond issued by a local bank and counter-secured by an international bank via a guarantee or standby letter of credit. The performance bond will often be payable locally against a bare statement of default and demand. The international bank counter-securing that bond will pay out against the local bank's bare statement that it has been obliged to pay. Short of proving the local bank to be fraudulent, the international bank has no option but to honour its obligations. Claims can in some cases be wildly disproportionate to any conceivable damage or loss. These excess claims are more likely to be motivated by commercial opportunism than criminality but it does demonstrate the limitations on a bank's ability to monitor the end purpose of every payment.

In the ICC's Global Trade and Finance Survey issued in 2014, 60 per cent of the respondents to the survey considered the lack of harmonisation of compliance standards created a significant challenge for the industry. Needless to say, several organisations such as The Wolfsberg Group and the FATF have as an objective the provision of international guidelines and practices for financial institutions in respect of anti-money laundering procedures and standards. However, these are only guidelines and are not an enforceable standard of practice.

In addition to the complexity and multiple laws and regulations applicable to trade finance transactions, it is noted by PwC in their report issued in September 2014[12] that there is also a lack of data-sharing between governmental authorities (customs, tax, and legal authorities). The report also mentions that the traditional, document-heavy approach in trade finance also hinders the ability to create reliable IT and data tools to counter money laundering and PwC expressly state that this approach 'promotes reliance on manual systems of investigation and analysis, which not only limits an institution's own statistical analysis but limits the potential to create timely, accurate reference data that could be shared with other parties to facilitate identification of trade based money laundering risks.'

Efforts focused on combatting money laundering in other sectors

Trade finance is not only attractive to money launderers due to its nature, but also because regulators and therefore financial institutions have been focusing efforts and staff to counter money laundering in sectors other than trade finance.

Methods used for trade-based money laundering

Money launderers use different techniques that evolve and adapt to the regulatory framework and the law enforcement environment in place, as well as to the type and the source of criminal property that is being laundered. For trade-based money launderers, either: (i) the importer/buyer and exporter/seller of the goods act in concert and are aware that the funds originate from illicit means; or (ii) only the exporter/seller or the importer/buyer is laundering money and the other is not aware that the funds are illicit – in which case the launderer is acting fraudulently towards the other party.

The current techniques used by trade based money launderers that have been identified are outlined in the following sections.

Under invoicing

A money launderer is under invoicing when the goods are exported at a value which is below the fair market value of the goods. Here, the importer/buyer will have an excess value when the importer/buyer re-sells the goods on the open market. This allows the exporter/seller of the goods to transfer funds to the country in which the importer/buyer of the goods is located.

Over invoicing

Over invoicing is the opposite of under invoicing where the goods are exported at a value which is above the market value of the goods so that the exporter/seller will have an excess value upon payment from the importer/buyer. This allows the exporter/seller of the goods to receive funds from the country in which the importer/buyer is located. An example reported by the JMLSG is the case of a West African businessman receiving transfers from several business entities based in Europe of approximately US$7m and linked to the fishing industry, during a three-year period. The transfers out of the account of approximately US$4m over the same period were made to various businesses in the maritime industry. The analysis carried out showed that the income of the West African entities was 'grossly disproportionate to reported sales' and that one of the business partners was suspected of money laundering in Italy.[13]

Multiple invoicing

This is the case where more than one invoice is issued for the same goods whereby the exporter/seller can justify the receipt of multiple payments from the importer/buyer for the same shipment. These payments become even more difficult to track and monitor when they are made by more than one party (for example, the importer/buyer and a possible guarantor or through their banks by documentary credit) and for multiple legitimate reasons (for example,

amendment of payment terms, payment of default interest for delay in delivery, or difference in interest rate).

Over shipment
In this case, the seller/exporter delivers more goods than the quantity or quality (or both) of the goods detailed in the invoice. Here the value of the goods is misrepresented in the shipping documents. This allows the exporter/seller to transfer excess value to the importer/buyer which the importer/buyer can convert to clean funds.

Under shipment (also known as 'short shipping')
This is the opposite to over shipment where the seller/exporter delivers less in goods than the quantity or quality (or both) of the goods detailed in the invoice, allowing the exporter/seller to receive excess funds from the importer/buyer.

Phantom shipments
This is the extreme case of under shipment where no goods are shipped and all shipping documentation is falsified. An example is where one of the methods used was to provide false invoices of precious metals which never reached the country of the importer, as in the case reported by the JMLSG of silver and gold smuggling for the purpose of VAT evasion and money laundering. In this case, the total amount of funds involved was USD$101m. Fifteen suspects were arrested, four of whom were charged with money laundering offences.[13]

False or misleading description of traded goods
This technique involves falsifying information on the transaction documents or in relation to the type or the source of the goods traded so as to mislead the other parties and avoid any suspicion (i.e. dual purpose goods – see the information on proliferation financing which will be covered in Chapter 5).

In using the methods above, money launderers also use other techniques that facilitate the money laundering process in trade finance transactions some of which are as follows:

- The use of front companies and shell companies: This technique consists of masking illicit funds behind businesses that conduct legitimate business activities generating legitimate business profits. This technique of hiding behind a corporate identity is used by money launderers in all sectors and such businesses are usually set up in tax havens with strong regulations on bank secrecy.
- The use of funnel accounts: In this case, the money launderer deposits the funds in one geographical area (often in amounts below the cash reporting threshold) which are then withdrawn in a different geographical area.

- The use of barter transactions: These transactions involve the exchange of goods, one for another. Please see the example of the diamond market in Chapter 5.
- Lightly regulated countries and free trade zones: These countries and zones are attractive to money launderers as they are easy places to set up legal entities, to avoid or bypass custom controls, and to undertake operations in which goods are transformed or used to produce other goods (i.e. dual use goods).

Preventive measures to counter money laundering in trade finance

In order to be proactive, stay ahead of the overflow of regulatory reform and to mitigate the risks associated with money laundering in trade finance, financial institutions and trade organisations need to, amongst other things, design and implement risk-based monitoring and customer due diligence procedures within their policies and training. Not all financial institutions are currently performing to the standard required by the regulators in the UK, as illustrated in the FCA's review of a panel of international banks' procedures in determining risks in the trade finance sector and the examples of poor due diligence practice exhibited.[15]

In line with the obligations set out in the Money Laundering Regulations 2007, the JMLSG guidance sets out not only the general obligations of financial institutions and further advice in respect of their risk-based procedures and policies, but also sector specific guidelines on such policies and procedures. The main obligations and advice set out in the JMLSG guidance specific to the trade finance sector are covered in the following sections.[16]

The ability to assess the risk

The starting point for a risk-based approach is that the customer is not a money launderer and that criteria to be established in the firm's policy should indicate whether a customer presents a higher risk. Higher risk must be escalated to senior management.

Customer due diligence

Due diligence is to be undertaken on the customer who is the instructing party for the purpose of the transaction. It is often the case that, for trade finance transactions, the customer is already a customer of the bank where due diligence has already been carried out and where the bank is to assess whether further due diligence is required. It is recommended that due diligence on the other parties should be carried out – the extent of such due diligence should be contained in the firm's written policy but should be more or less

extensive depending on which capacity the financial institution is acting in, to the amount of information the financial institution has access to, and if enhanced customer due diligence is required (in correlation to the risk involved).

Different capacities of the financial institution in a trade finance transaction
The instructing party, on which customer due diligence is to be carried out by firms, will depend on the role of the firm in the transaction and the instruments that the bank is providing[17]:

- Import (outward) LC – The instructing party for the issuing bank is the applicant;
- Export (inward) letters of credit – The instructing party for the advising/confirming bank is the issuing bank. Firms should follow the specific guidance provided by the JMLSG on correspondent banking;
- Outward collections – The instructing party is the customer/applicant;
- Inward collections – The instructing party is the customer/applicant; and
- Bonds/guarantees – The instructing party is either the customer, correspondent bank, or another third party.

Forfaiting transactions
Forfaiting is a method of trade finance that allows the exporter to transfer account receivables at a discount to financial institutions in consideration for cash on a 'without recourse' basis. In this case, the instructing party will normally be the exporter on whom due diligence should be carried out. The firm should also carry out due diligence on the other parties to the transactions, such as the importer and the transaction documents to ensure the validity of the transaction.

Enhanced due diligence
When the transaction presents a higher risk based on the firm's risk assessment of the transaction (i.e. types of customers, countries in which the trade is involved, type of goods etc.), customer due diligence should be undertaken as per the above but with additional checks that will enable the bank to fully understand the commercial aspects of the transaction and to be fully assured of the legitimacy of the transaction. Examples of the additional checks are as follows[18]:

- Enquiries into the ownership of the other parties of the transaction;
- Obtaining information from the instructing party on the frequency of trade and the quality of the business relationship between the parties;
- Checking the ICC International Maritime Bureau for warning notices; and
- Referring the transaction to external agencies such as the ICC Commercial Crime Services.

Screening

This is dealt with in Chapter 5.

Monitoring

Financial institutions are under an obligation to report suspicious transactions. In their general monitoring, financial institutions usually use the following information to flag suspicious transactions[19]:

- Payment values;
- Volume of payments;
- Countries of payment;
- Originator and beneficiary;
- Patterns based on the country or entity involved; and
- Volume of shipments.

The depth and frequency of the monitoring depends on the risk analysis of the business/transaction/parties involved. In any event, structured controls and procedures for monitoring purposes should be included in firms' policies.

Training of staff

Firms must hire staff with a high level of understanding of the trade finance sector, including export licence regimes and authorisations of trading. The staff need to receive regular training outlining both how trade finance transactions can be used by money launderers, and how to understand and manage the risk. It is stated in the JMLSG guidance that training programmes should refer to the FATF's red flags that are generally directed to governmental agencies but can be useful also in the private sector. The FATF red flags can be found in Annex 15-V of Chapter 15 of Part II of the JMLSG Guidance, a few examples of which are as follows:

- Significant discrepancies between the description of the commodity on the bill of lading and the invoice;
- Significant discrepancies between the description of the goods on the bill of lading (or invoice) and the actual goods shipped; and
- Inconsistency between the size of the shipment and the scale of the exporter's or importer's regular business activities.

The current situation

In the trade finance sector, KPMG noted a significant divergence in practice between US banks and those based in Western Europe and other regions in terms of both the use of existing customer information across bank departments and the independent verification of trade documentation to identify potential

money laundering transactions. A lack of tailor-made anti-money laundering training for the trade finance sector has also been highlighted. All these factors have raised the profile of trade finance with regulators, and banks can expect increased attention from the authorities.

An example of non-compliance was the case of Standard Bank where the FCA's first notable fine was issued in January 2014 (£7.6m) because the bank's policies for preventing money laundering were not in practice being applied with consistency – particularly with regard to PEPs (politically exposed persons) and those corporates associated with them.[20] In the US, meanwhile, Standard Chartered Bank was on the receiving end in August of a US$300m fine from the New York State Department of Financial Services for failure to adhere to remedial measures it had undertaken to put in place in relation to its anti-money laundering procedures following an earlier investigation and fine by the same authorities in 2012.[21] The message appears to be that the regulators are beginning to target non-compliant players in the trade finance sector.

To emphasise their focus on the trade finance sector, in June 2014 the FCA published an amended version of its 2013 Financial Crime Guide together with the results of its survey of a number of banks active in the trade finance sector handily titled 'Examples of good and poor practice in Banks' control of financial crime risks in trade finance'.[22] The new guidance took effect on 12 June 2014. The section on anti-money laundering policies and training reveals that some banks at least are still not picking up on the theme of trade finance specific policies and training which have been flagged up by the regulators previously. Some of the findings of 'poor' practice make worrying reading.

The obligations on banks to risk assess, carry out both simple and enhanced due diligence, and continually monitor the customers who they bank is a costly burden. In the 2014 ICC Banking Commission Global Survey, firms indicated that the main restriction to developing their trade pipeline was the burden of compliance. In order to develop the market but at the same time counteract against money laundering and terrorist financing, a balance needs to be found by the industry players in the industry in the implementation of appropriate procedures that do not reduce the appeal of the trade finance market.

As mentioned in the paragraph on 'Lack of harmonisation' above, and as noted by international regulatory bodies and authorities, another solution to the problem of money laundering in the trade finance sector would be more significant intervention at state level that would provide a reasonable global price benchmark for products. PwC states that price benchmarks for products between countries will provide invaluable data to counter money laundering. A harmonised 'method for detecting and identifying trade-based money laundering is the analysis of import and export data between countries at macro level.'[23]

References

1. FATF, 'What is money laundering?', see: www.fatf-gafi.org/pages/faq/moneylaundering/.
2. See: www.imf.org/external/np/speeches/1998/021098.htm.
3. As set out in the JMLSG Guidance at: www.jmlsg.org.uk/.
4. See the JMLSG Guidance.
5. An organisation of international and market leading banks engaged in correspondent banking business such as, amongst others, Banco Santander, Citigroup, Credit Suisse, Deutsche Bank, Goldman Sachs, and Barclays. See www.wolfsberg-principles.com.
6. The relevant guidelines of The Wolfsberg Group are the 'Wolfsberg Trade Finance Principles' (see www.wolfsberg-principles.com/pdf/standards/Wolfsberg_Trade_Principles_Paper_II_(2011).pdf) and the 'Wolfsberg Anti-Money Laundering Principles for Correspondent Banking' (see www.wolfsberg-principles.com/pdf/home/Wolfsberg-Correspondent-Banking-Principles-2014.pdf).
7. The Wolfsberg Group, 'The Wolfsberg Trade Finance Principles (2011)'. See: www.wolfsberg-principles.com/pdf/standards/Wolfsberg_Trade_Principles_Paper_II_%282011%29.pdf.
8. See: www.gfintegrity.org/reports/.
9. See 'Goods gone bad', at: www.pwc.be/en/publications/2014/money-laudering.jhtml.
10. See: www.wto.org/english/news_e/pres14_e/pr721_e.htm.
11. See: www.iccwbo.org/Products-and-Services/Trade-facilitation/ICC-Global-Survey-on-Trade-Finance/.
12. See 'Goods gone bad', at: www.pwc.be/en/publications/2014/money-laudering.jhtml.
13. See: www.jmlsg.org.uk/other-helpful-material/article/front-companies.
14. See: www.jmlsg.org.uk/other-helpful-material/article/silver-and-gold-smuggling.
15. FCA, 'Banks' control of financial crime risks in trade finance', July 2013. See: www.fca.org.uk/static/documents/thematic-reviews/tr-13–03.pdf.
16. For further detail on the obligations and guidelines, please refer directly to the JMLSG Guidance.
17. Please refer to the JMLSG Guidance for more information on the extent of customer due diligence to be undertaken.
18. List provided in the JMLSG Guidance.
19. List provided in the JMLSG Guidance.
20. See: www.fca.org.uk/news/standard-bank-plc-fined-for-failures-in-its-antimoney-laundering-controls.
21. See: http://online.wsj.com/articles/n-y-financial-watchdog-fines-standard-chartered-300-million-1408466076.

22. This can be found at http://fshandbook.info/FS/html/FCA/FC/link/PDF.
23. See 'Goods gone bad', at: www.pwc.be/en/publications/2014/money-laudering.html.

Chapter 5: Terrorism financing

By Robert Parson, partner, and Imogen Holmgren, trainee, Reed Smith LLP

TERRORISM IS defined in Section 1 of the Terrorism Act 2000 (TACT) as, amongst other things, 'the use or threat of action… designed to influence the government or an international governmental organisation, or to intimidate the public… [which is made] for the purpose of advancing a political, religious or ideological cause… [and which involves] serious violence against a person… or serious damage to property, endangers a person's life… or creates a serious risk to the health or safety of the public… or is designed seriously to interfere with, or seriously to disrupt, an electronic system.'

The TACT sanctions and punishes acts of terrorism, and it also criminalises the financing of terrorism. Under Schedule 7 of the Counter-Terrorism Act 2008 (CTA), terrorist financing is defined as the 'use of funds, or the making available of funds, for the purpose of terrorism, or the acquisition, possession, concealment, conversion or transfer of funds that are (directly or indirectly) to be used or made available for those purposes'.

There are many similarities between the act of laundering criminal property and the movement of funds on the one hand, and the act of financing terrorist activities on the other. However, the main differences between the two lie in the fact that the funding of terrorism is, in general, more difficult for financial institutions to detect and prevent because:

- Terrorism financing is a broad term encompassing any financing of terrorist activity which could involve small amounts to finance a single terrorist act or the flow of a significant amount of funds financing the infrastructure of major terrorist organisations such as Al Qaeda. The difference in terms of funds flow makes it difficult to detect and prevent compared to money laundering which tends to consist of significant individual amounts of funds laundered; and
- Unlike money laundering, terrorism can be and often is financed by apparently legitimate sources such as charitable donations, and it is difficult for the actors in the financial sector to determine at which point those funds cease to be legitimate and are therefore determined to be funds intended for financing terrorism. In the past, organisations such as Sanabel Relief Agency, which was registered with the UK Charity Commission, were

subsequently found to be fundraising fronts for Al Qaeda and other terrorist organisations.

Terrorism financing offences and obligations relevant to the trade finance sector

Similar in a sense to the anti-money laundering regime, the measures countering terrorism financing applicable to financial institutions in the UK are extensive and can be found across a range of sources (legislation, regulation, rules, and guidelines). The anti-money laundering regime and the counter terrorism regime go hand in hand and therefore several key elements of the applicable framework for countering money laundering that are currently in place in the UK are the same for countering terrorism financing. The key elements for countering terrorism financing are the following:

- TACT;
- CTA;
- The Terrorist Asset Freezing etc. Act 2010 (TAFA);
- The Money Laundering Regulations 2007;
- HM Treasury Sanctions Notices and News Releases; and
- The FCA Handbook.

Money laundering related offences relevant to the trade finance sector

Several offences related to terrorism financing exist, and the main offences that are applicable to the trade finance sector are contained in TACT. The legislation states that any person who:

- Invites another person to give and provide money or other property, or is engaged in the sole action of receiving money or other property with the intention for it to be used, or has reasonable cause to suspect that it may be used, for the purpose of terrorism. It is also considered an offence to provide any asset with the knowledge (or reasonable suspicion) that it will or may be used for the purpose of terrorism (section 15);
- Uses money or other property for the purpose of terrorism or possessing such money or other property with the intention for it to be used (or reasonably suspects that it may be used) for the purpose of terrorism (section 16);
- Enters into or is concerned in an arrangement resulting from which money or other property is made or is to be made available to another with the knowledge (or reasonable suspicion) that it will or may be used for the purposes of terrorism (section 17);

- Enters into or is concerned in an arrangement which facilitates the retention or control by or on behalf of another of terrorist property by concealment, removal from the jurisdiction, transfer to nominees, or in any other way. This offence will not be charged if it is evident that the alleged offender had no knowledge (or reasonable cause to suspect) that the arrangement related to terrorist property (section 18); and
- Fails to comply with the duties of disclosure of any offence under the above that the person believes or suspects that another has committed (section 19).

TACT provides that a court is to take into account any relevant guidance issued by a supervisory authority or other regulatory body and approved by HM Treasury when considering whether an alleged offender failed to report under TACT. Guidance has been approved by the Joint Money Laundering Steering Group (JMLSG).

Other than the offences under TACT:

- The CTA grants HM Treasury power to issue directions by which the Treasury may impose additional requirements to be complied with (e.g. additional due diligence, monitoring, or reporting measures) in entering into or pursuing transactions or business relationships with a person carrying out business in the country, with the government of the country, or with a person resident or incorporated in the country concerned by the direction. The Treasury may only issue directions if all conditions of Section 1 of Schedule 7 of the CTA are met (e.g. that the Financial Action Task Force (FATF) has advised that measures should be taken in relation to the country because of the risk of terrorist financing or money laundering); and
- The TAFA grants HM Treasury power to freeze assets in the event of an offence committed pursuant to Section 11 of TAFA. Section 11 provides that one must not deal with funds or economic resources owned, held, or controlled by 'designated persons' or make funds, economic resources, or financial services available to or for the benefit of such persons. Under TAFA, a 'designated person' is referred to as a person designated by the Treasury or a person that is included in the list provided for by Article 2(3) of Council Regulation 2580/2001. The Treasury may make final or interim designations under the conditions set out in Section 2 of the TAFA (e.g. if they reasonably believe the person is or has been involved in terrorist activities).

Other initiatives

EC Regulation 881/2002 imposes specific restrictive measures directed against persons associated with the Al-Qaeda network, including flight bans

and the freezing of funds and other financial resources regarding the Taliban in Afghanistan. Several organisations also provide general and sector specific guidelines and recommendations on ways to prevent terrorism financing. For example:

- FATF issues the 'International Standards on Combating Money Laundering' and the 'Financing of Terrorism and Proliferation' which has as its goal to provide minimum international standards for action to ensure that the efforts to prevent money laundering are applied consistently at an international scale.
- The Counter-Terrorism Implementation Task Force (CTITF) of the United Nations has provided a number of reports such as the 'CTITF Working Group Report' in which it provides general principles for combatting terrorism financing for the public and private sector.[1] Although it stresses the importance of combatting terrorism financing, it also states that 'authorities should exercise caution not to introduce laws or regulations burdening private and public sector stakeholders in the name of countering the financing of terrorism without sufficient evidence or typologies that the burden is proportionate to the risk'. In this report, CTITF also shares its findings one of which is that financial institutions usually comply with the general reporting anti-money laundering/counter terrorism financing requirements, but no in-depth research has been carried out as to the methods specifically used by persons intending to finance terrorism and that there are few specific indicators available other than sanction indicators for financial institutions to assess the risk of terrorism financing.
- The World Bank and the International Monetary Fund issued a 'Reference Guide to Anti-Money Laundering and Combating the Financing of Terrorism' in which it provides guidelines for countries to implement a regime that complies with international standards.[2]

The Money Laundering Regulations 2007 and the FCA Handbook

The Money Laundering Regulations 2007 and the Financial Services and Markets Act 2000 ('FSMA') also apply to terrorism finance. In this respect, players in the trade finance sector are obliged to establish and maintain adequate and appropriate risk-based policies and procedures to prevent terrorism financing which must cover customer due diligence, reporting, record-keeping, internal control, risk assessment and management, compliance management, and communication.

Furthermore, under FSMA, the Financial Conduct Authority (FCA) may initiate proceedings for offences under prescribed regulations relating to terrorism financing where the failure to comply with the requirements of the

Money Laundering Regulations 2007 constitutes an offence, in which case the standards and practices set out in the FCA Handbook of rules and guidance are also applicable. FCA-regulated firms and 'approved persons' are therefore required to implement appropriate systems and controls over the management of terrorism financing risks.

Money laundering in trade finance

For the same reasons described in Chapter 4 in relation to money laundering, the trade finance market is also attractive to financiers of terrorism. Although money laundering and terrorism finance are different in terms of their aims, the methods used by money lauderers are the same for persons wishing to finance terrorism via trade transactions.

Proliferation financing

There is currently no agreed legal definition of 'proliferation financing', but the working group at the FATF proposed the following definition: 'the act of providing funds or financial services which are used, in whole or in part, for the manufacture, acquisition, possession, development, export, trans-shipment, brokering, transport, transfer, stockpiling or use of nuclear, chemical or biological weapons and their means of delivery and related materials (including both technologies and dual use goods used for non-legitimate purposes), in contravention of national laws or, where applicable, international obligations'. This definition refers to the notion of 'dual-use goods' which are goods that can have both a commercial and a military purpose. Numerous international and European sanctions are currently in place for dual-use goods.

Examples of terrorism financing through trade

Tobacco smuggling

In 2002, a suit was filed by the European Community against an American tobacco company alleging money laundering activities surrounding cigarette smuggling. It was suspected that the proceeds from the smuggling of cigarettes from Turkey, through the Northern border of Iraq, and into two PKK controlled areas of Iraq (allegedly violating trade embargoes in Iraq) were used to fund terrorist activities of the PKK and other terrorist organisations operating in Northern Iraq.[3]

In 2004, ten people were arrested for smuggling more than US$2m in contraband cigarettes from Virginia to New York. One subject was arrested in Detroit and found with hundreds of thousands of dollars in wire transfer receipts showing payments to people associated with Hezbollah.[4]

Sugar trade

Allegations have been widely published to the effect that sugar exported from Somalia to Kenya illegally is funding the terrorist group Al-Shabaab.[5]

The production and refining of oil

ISIS is believed to control some 60 per cent of Syria' oil fields and have established export routes – including across the Turkish border – to raise finance for their terrorist activities.[6]

The diamond trade

The FAFT and the Egmont Group of Financial Intelligence Units have recently produced a report on 'Money Laundering and Terrorist Financing through Trade in Diamonds'.[7] In this report, it points out that the diamond market has vulnerabilities that can be used and exploited by money launderers and persons wishing to finance terrorism. Examples of such vulnerabilities are:

- The global nature of the trade;
- The fact that diamonds can also be used as currency;
- That it is difficult to produce a price benchmark;
- That it is a specialised market where law enforcement authorities and financial institutions do not necessarily have the requisite knowledge or level of awareness; and
- The characteristics of the product (small in size and in weight so easily transportable and of high worth where one stone can reach more than US$20m).

This report concludes that 'diamonds could therefore be used to finance terrorism in a scenario where a donor or financier purchases diamonds legitimately, using lawfully derived funds, and then transfers the diamonds to a terrorist or terrorist organisation who exchange the diamonds for equipment or cash intending to finance terrorist activities.'

Preventive measures to counter terrorism financing in trade finance

The prevention measures employed in trade finance transactions to counter money laundering are the same as those employed to counter terrorism financing.

With regards to preventive measures against proliferation financing, it is extremely difficult for firms to monitor and determine which dual-use goods are used for proliferation due to the highly specialised knowledge and experience needed to determine if such goods are to be used for proliferation purposes,

and due to the very few transactions and customers in this type of illicit transaction. Nevertheless, FATF published reports in 2008 and 2010[8] which assess the risk of financial institutions being involved in such transactions.

With regards to sanction checking within financial institutions, the FCA, in its amended version of its 2013 Financial Crime Guide, pinpointed failures seen in trade finance banks in relation to sanctions checking, and it noted the following key areas of concern:

- Staff dealing with trade-related sanctions queries who are not appropriately qualified and experienced to perform the role effectively;
- A failure to screen trade documentation;
- A failure to screen against all relevant international sanctions lists;
- A failure to keep up-to-date with the latest information regarding name changes for sanctioned entities, especially as the information may not be reflected immediately on relevant sanctions lists;
- A failure to record the rationale for decisions to discount false positives;
- A failure to undertake risk-sensitive screening of information held on agents, insurance companies, shippers, freight forwarders, delivery agents, inspection agents, signatories, and parties mentioned in certificates of origin, as well as the main counterparties to a transaction; and
- A failure to record the rationale for decisions that are taken not to screen particular entities and retaining that information for audit purposes.

The FCA's emphasis on the fact that banks should not confuse money laundering risks with sanctions risks comes, of course, at a time when banks are stretched in dealing with the increasing volume of sanctions related to the Crimea/Ukraine crisis. Of course resources within the law enforcement agencies, regulators, and the banks themselves are not limitless. With well in excess of 200,000 Suspicious Activity Reports (SARs) being sifted through by the authorities every year, it is clear that parties to trade transactions take money laundering reporting obligations seriously. It remains to be seen whether that level of risk assessment and performance of anti-money laundering obligations will satisfy a regulator keen to establish zero tolerance towards money laundering and terrorist financing.

References

1. See: www.un.org/en/terrorism/ctitf/wg_financing.shtml.
2. See: http://web.worldbank.org/WBSITE/EXTERNAL/TOPICS/EXTFINANCIALSECTOR/EXTAML/0,,contentMDK:20746893~menuPK:2495265~pagePK:210058~piPK:210062~theSitePK:396512,00.html.

3. Source: *EC v RJ Reynolds* (30 October 2002), EC v RJ *Reynolds, Phillip Morris* (1 February 2002).
4. See: www.washingtonpost.com/wp-dyn/articles/23384-2004Jun7_2.html..
5. See: http://sabahionline.com/en_GB/articles/hoa/articles/features/2013/04/24/feature-01.
6. See: www.ibtimes.co.uk/iraq-crisis-isis-sells-stolen-crude-oil-raising-over-1-million-per-day-1462389
7. See: www.fatf-gafi.org/documents/news/ml-tf-through-trade-in-diamonds.html.
8. See: www.fatf-gafi.org/topics/financingofproliferation/documents/typologiesreportonproliferationfinancing.html. See also: www.fatf-gafi.org/media/fatf/documents/reports/Status-report-proliferation-financing.pdf.

Chapter 6: Sanctions and trade finance

By Emma Radmore, managing associate, and Christina Pope, trainee, Dentons

SANCTIONS CONCERNS are common in trade finance. Trade finance may involve designated persons or goods, and it often uses irrevocable instruments such as demand guarantees and letters of credit. Firms in the trade finance sector need to manage their sanctions risk both at the outset of a contract or relationship and on an ongoing basis. Sometimes they may face a stark choice of breaching sanctions or breaching the contract. They should therefore analyse their legal position when agreeing documents to manage this risk.

This chapter explains what sanctions may be relevant in the trade finance sector. It is written from a UK legal perspective with particular reference to the regulatory requirements that apply to trade financiers operating in the UK and authorised under the UK Financial Services and Markets Act 2000. UK sanctions laws, however, apply more widely, covering not only any UK firm but also anyone doing business in the UK. This chapter does also refer to the importance of other sanctions, particularly those imposed by the US. It assesses the impact of these sanctions and considers what trade finance firms can do to protect themselves.

What are sanctions?

Sanctions are legal measures designed to impose restrictions on dealings with countries, governments, entities, or individuals in an attempt to influence a change in policy or actions, or as an enforcement tool to align compliance with international legal or diplomatic standards. The international community uses sanctions, in particular, when there is a perceived risk to global peace and security, including terrorism and illicit financing.[1]

Sanctions broadly sit in two categories: financial sanctions, which seize and restrict availability of funds, and trade sanctions, which impose embargoes on certain goods or services.

Financial sanctions

Depending on the policy stance or actions they aim to address, financial sanctions can include:

- An outright ban on any inward or outward funds transfer (or transfers allowed subject to notification and/or licences);
- An asset freeze;
- Limits on trading;
- Investment bans; and
- Most recently, restrictions on capital market activities.

Financial sanctions could target any person or organisation in a given country, or they could be limited, for example, to governments or to named entities and individuals designated by the particular sanctions regime. Sanctions are invariably targeted at named entities and individuals. From a European perspective, Iranian sanctions are the exception to this general rule.

Trade sanctions

The most often applied trade and other sanctions measures are:

- Embargoes on exporting or supplying arms and associated technical support, training, and financing;
- A ban on exporting equipment that might be used for internal repression;
- Financial sanctions on individuals in government, government bodies, and associated companies, or terrorist groups and individuals associated with those groups;
- Travel bans on named individuals; and
- Bans on imports of raw materials or goods from the sanctions target.

Where do UK sanctions come from?

Sanctions that apply under UK law usually stem from decisions of the EU (which in turn derive from recommendations of the United Nations (UN) Security Council) and from autonomous UK government decisions. The sanctions are contained in secondary legislation (with a few exceptions discussed below). UN Recommendations are not directly applicable to businesses in any jurisdiction until implemented by their governments into national law. It is, nevertheless, useful for firms active in sensitive industries or jurisdictions to be aware of UN Recommendations, to give themselves time to prepare for national implementation – which can sometimes follow very quickly.

The EU makes its financial sanctions by Regulations, which are directly applicable to individuals and businesses within Member States. The UK

Government (in the form of HM Treasury (Treasury)), however, makes secondary legislation that sets out both the scope of the sanctions and the consequences of breach. Separately, the UK makes its own sanctions under the Terrorist Asset Freezing, etc. Act 2010 and there is, to some extent, also an overlap with directions the Treasury makes under the Counter-Terrorism Act 2008.

As of November 2014, the UK had in place financial sanctions affecting nearly 30 jurisdictions and regimes.[2] The Treasury constantly updates lists of all entities and individuals who are designated under the various sanctions. These are Designated Persons, and the Treasury keeps lists by regime, and on one combined list known as the Consolidated List.[3] This Consolidated List includes all names sanctioned under EU Regulations and persons designated under the Terrorist Asset Freezing, etc. Act. The Treasury keeps a separate list of entities subject to restrictions on capital raising under the Ukraine sanctions,[4] and yet another setting out Directions under the Counter-Terrorism Act and Financial Task Force advisories. Although the Counter-Terrorism Act and Financial Task Force advisories relate mainly to money laundering risks, they will also be relevant to firms' sanctions compliance.

The lists of Designated Persons for each relevant regime vary widely in both numbers of names on the list and frequency of updates. Certain lists bear few names and have not been updated for some time. Others (chiefly those relating to Al-Qaida, Terrorism and Terrorist Financing, Ukraine, Syria, and Libya) bear more names and/or are updated regularly.

UK Trade Sanctions also stem from UN and EU laws, and are usually implemented into UK law by amendment to the Export Control Order 2008. The Department for Business, Innovation and Skills (BIS) administers trade sanctions, including export controls and arms embargoes, through the Export Control Organisation (ECO). It separately lists jurisdictions and regimes towards which various trade sanctions apply. The lists, like the Consolidated List, constantly change.

Who must comply?

All individuals and legal entities incorporated under the laws of any part of the UK or who are in the UK must comply with UK and EU sanctions. British nationals or legal entities who are established under English law, but run their business outside of the UK, must also comply with UK and EU sanctions.

In principle, therefore, the UK sanctions regime applies to anyone incorporated in the UK (including overseas branches) or any British national, wherever they are. It does not apply to subsidiaries of UK companies which are incorporated and run outside the UK.

International sanctions

Businesses and individuals in the UK may also be subject to the sanctions regimes of other jurisdictions, such as those of the US Office of Foreign Assets Control (OFAC).[5] For instance, UK branches of US businesses must comply with both UK and US sanctions regimes, as will US nationals working in the UK. Similarly, US branches of UK entities will be subject to both sets of sanctions. Increasingly, large financial institutions find they have no practical choice but to implement a group-wide financial crime compliance policy that requires all entities within the group to comply with sanctions relevant to any one or more entities within the group.

Also, parties may be asked to comply with third party country laws or a particular transaction may fall under a third country sanction due to its nature. For example, the parties transact in a currency of a state which has a sanction in place for the counterparty or beneficiary. US sanctions are particularly relevant, not least because many transactions are denominated in US dollars and therefore at some point will involve a US bank which is subject to the US sanctions regimes even if other participants are not. The scope of US sanctions is also so wide that it can at times catch businesses with no US link, especially if their actions cause a US entity to breach US sanctions.

It is outside the scope of this chapter to discuss sanctions imposed by jurisdictions outside the UK, but firms must be aware of those relevant to them and factor into their compliance programmes the requirements and risks these sanctions present. The many, large fines the US enforcement authorities have imposed on international banks for breach of US sanctions and anti-money laundering laws (most recently BNP Paribas) underline the importance of taking a holistic jurisdictional approach to risk management and compliance.

What do UK financial sanctions restrict?

The existence of a sanctions regime does not of itself prevent all dealings with any person in, or related to, the particular jurisdiction or regime. Instead, each regime will bar all, or specific, dealings with any individual or entity that is a Designated Person or is owned by a Designated Person, or that will be for the benefit of a Designated Person.

Each financial sanctions regime has its own scope. However, several features are common to most regimes. The sanctions:

- Apply to dealings with 'Designated Persons';
- Apply to 'funds' which are, broadly, any financial asset or benefit. Not just cash or payment instruments, but also letters of credit, export financing instrument, bonds or other financial commitment and securities;

- Apply to 'economic resources' which are any assets which can be used to get funds, goods, or services;
- Cover both direct and indirect dealings; and
- Cover actions taken deliberately to avoid sanctions.

There are several offences and obligations created by UK Statutory Instruments for each regime. However, in general, under each instrument it is a criminal offence for any UK national or UK incorporated body, or any other person in the UK (a UK Person) to:

(a) Deal with funds or economic resources belonging to, or owned, held or controlled by, a Designated Person;
(b) Make funds available, directly or indirectly, to a Designated Person;
(c) Make funds available to any person for the benefit of a Designated Person. Funds are considered to be 'made available' for the benefit of the designated person only if that person gets, or may get, a significant financial benefit;
(d) Make economic resources available, directly or indirectly, to a Designated Person;
(e) Make economic resources available to any person for the benefit of a Designated Person. Economic resources are considered to be made available for the benefit of a designated person only if that person gets, or may get, a significant financial benefit;
(f) Intentionally engage in activities knowing the object or effect of them is (whether directly or indirectly);
    (i) to avoid the prohibitions in (a) to (e) above; or
    (ii) to enable or facilitate the contravention of these prohibitions.

For offences (a) to (e), the offence is committed where the UK person knows, or has reasonable cause to suspect, its actions will constitute the offence.

Any UK person who finds themselves in possession of funds or economic resources held or controlled by a Designated Person must freeze them in an appropriate bank account. Banks must notify Treasury of frozen funds they receive. Any UK person wishing to deal with a Designated Person, or to continue to deal with a person who has become a Designated Person, may apply to Treasury for a licence to do so. Whether this licence will be granted depends on a number of factors.

Banks also have a duty to report relevant information to Treasury and respond to Treasury enquiries. Failing to do so, or misleading Treasury, is also a criminal offence.

As well as these general restrictions on dealings with Designated Persons and persons related to them, there are further restrictions for some regimes, notably the one for Iran. Although restrictions against Iran have been relaxed to some extent, the UK government does not encourage trade with, or investment in, Iran and has withdrawn commercial support for trade. It advises companies that any trading with Iran is done at their own risk. Where banks choose to trade with Iranian entities, they must be aware of the added restrictions that sanctions impose on the Iranian banking sector specifically, and on any transfers of money to or from Iranian persons.

In relation to Ukraine, the EU introduced separate sanctions that restrict named state-owned Russian banks and their subsidiaries, and specified oil and defence entities from accessing EU primary and secondary capital markets or the loan markets. While these entities are not Designated Persons for the purposes of the asset freeze, UK trade financiers must consider their position under this separate regime also if doing business with any of these entities. US law introduced similar, but not identical, restrictions.

What do UK trade sanctions restrict?

Arms embargoes are imposed by the UN or EU on 'arms and related material' (such as military ammunition, weapons, and goods). The UK typically interprets this as covering all goods and technologies on the UK Military List. Goods that are not specifically listed might also need a licence under the Military End-Use Control. Controls on the supply of military items between another third country and the sanctions target (trafficking and brokering) also apply. Certain specific sanctions are imposed on dual-use goods such as petrochemicals or telecommunications items.

It is a criminal offence to export, import, or trade in goods that are subject to a sanctions and embargo regime or which are dual-use goods without a specific licence from the ECO. The restrictions will extend to many financial services entities that may provide funding or insurance in relation to the goods. What licence is required depends on the goods, the jurisdictions in question, and the role of the entity. The ECO provides guidance to exporters and other firms on when a licence may be needed and what type of licence.[6]

Key practical issues: Financial sanctions

It can be difficult to assess whether UK financial sanctions bite where an entity subject to UK sanctions, A, is contracting or dealing with a person B who is not themselves a Designated Person, but who has a link by ownership with Designated Person C. It is not safe to assume that if the contracting party is not designated, then there is no problem. However, the link will not necessarily

mean the transaction cannot proceed. It is necessary to assess whether the nature of the link and of the contract mean there is a sanctions problem.

There are in fact several questions:

- Would the benefits B would derive under the contract constitute 'funds' or 'economic resources'?
- If the answer to the above is 'yes', would the funds or economic resources be made available to C?
- What degree of ownership and control is necessary between B and C for sanctions to bite on contracts with B?
- If the necessary ownership and control is present, would C get a significant financial benefit from using the funds or economic resources which A would be 'making available'?

Sometimes the answers to these questions will be obvious, but at other times the firm will need to carry out significant due diligence to form its view.

Key practical issues: Trade sanctions

The main problem trade financiers face in complying with trade sanctions is in the due diligence that is sometimes necessary to determine the possible and intended purpose of goods that are the subject of the finance. In the absence of clear guidance on the levels of expertise financiers are expected to have, applying a risk-based approach becomes essential, yet sanctions legislation does not expressly recognise such an approach.

Penalties

Each piece of sanctions legislation sets out the penalties for breach. In principle, there are no defences. There is no regulatory guidance or procedural requirements. On conviction a person will be liable to imprisonment (for periods up to seven years depending on the offence) and/or a fine. A breach of a sanction also carries personal liability for officers of the company, as well as the company itself. So far, the UK authorities have not shown great appetite for bringing sanctions prosecutions, and it is the US enforcement authorities who have imposed high fines on many international banks for sanctions (and sometimes also money laundering) offences.[7]

Role of the Financial Conduct Authority

In the UK, the more pressing fear for financially-regulated entities is the long arm of the Financial Conduct Authority (FCA). Banks offering trade finance services will fall within FCA's regulatory remit (even though they will be prudentially regulated by the Prudential Regulation Authority). Other firms may also,

depending on the precise activities they carry out. Almost every firm involved in the UK's trade finance sector will fall within the Money Laundering Regulations 2007 (MLR) and will need to be registered with FCA for MLR supervision if they are not authorised under the Financial Services and Markets Act 2000 (FSMA).

The FCA's objectives under FSMA include integrity, of which taking necessary action to prevent financial crime (including breach of sanctions restrictions) is one. The FCA has taken enforcement action against companies who have failed to put in place satisfactory systems and controls to prevent them being used by sanctions targets. It usually takes action for breach of Principle 3 of its Principles for Business, which states: 'A firm must take reasonable care to organise and control its affairs responsibly and effectively, with adequate risk management systems'. The rules in the senior management rules block of the Handbook also impose high level requirements on firms in relation to financial crime prevention. The FCA can also bring action for breach of the Money Laundering Regulations 2007 and, so far, has done this once, when it fined RBS for failure to have in place proper sanctions systems and controls – even though there was no evidence the bank had done business with any sanctions target.

Enforcement action by the FCA is a concern because the FCA's powers are sweeping, ranging from a fine (which will match the severity of the conduct, taking into account the financial position of the firm in question) to removal of a firm's authorisation. The FCA does not have to prove the firm has committed a criminal offence – just that its systems and controls were not adequate. Its other powers include taking the same range of actions against individuals within the firm who are approved persons and whose jobs meant they were complicit in, or should have spotted or acted to prevent, the conduct in question, and appointing third party experts to review and suggest improvements to a firm's procedures, at the firm's cost. So action by FCA creates both business, financial, and reputational concerns.

Firms should take careful note of both the sanctions guidance that forms part of the Joint Money Laundering Steering Group (JMLSG) Guidance notes[8] and also, in particular, the FCA's Financial Crime Guide (FC).[9] The FC is not binding guidance, but the FCA intends firms to use it in a proportionate way, and build its recommendations into their risk-based approach to compliance. It gives examples of good and poor practice which may be of help to firms, and backs up its guidance with thematic reports.[10]

While no chapter of the FC should be read in a vacuum, Chapter 7 of the guide is devoted to sanctions and asset freezes. It provides guidance to firms on:

- Governance;
- Risk assessment;
- Screening against customer lists;

- Matches and escalation; and
- Weapons proliferation.

The FCA and its predecessor have also carried out both general and trade-finance specific reviews into how banks comply with their sanctions obligations, including a 2013 review on trade finance business.[11] Firms should not ignore FCA guidance and should be prepared to justify instances where their policies and procedures depart from it.

Sanctions clauses in trade finance related contracts

Sanctions operate as a matter of law, irrespective of the terms of a contract. So, if sanctions prohibit taking certain actions, then the contract cannot be honoured. In the trade finance context this may lead, for example, to a payment not being made under a guarantee or letter of credit.

Financiers have sometimes included what have become known as 'sanctions clauses' in their transaction documents. Mostly this is because they are: (a) concerned about their position; and (b) it is a means of telling counterparties that they are subject to sanctions laws. However, it is also sometimes used as a method to attempt to get counterparties to comply with sanctions laws that would not otherwise apply to them. Sometimes these clauses can cause problems, not least because it can (especially for Cuban sanctions) be an offence for an EU entity to agree to comply with US sanctions where the EU entity is not legally obliged to do so.

The International Chamber of Commerce (ICC) has issued guidance on this point.[12] The guidance states that informative clauses – merely stating the bank's obligation to adhere to applicable laws on sanctions – are acceptable. However, it says parties must avoid including clauses which go beyond the scope of the applicable laws and regulation. The danger of doing so is that financiers may create a discretionary obligation in a contract which should be irrevocable.

Checklist for trade finance firms

Clearly each business has its own business model. But key to any sanctions compliance and protection programme must be:

- Appreciation from the board of the importance of sanctions compliance and allocation of appropriate resources, both human and financial;
- Assessment of the areas of business that present the most risk from sanctions restrictions – products, geographies, and customers/counterparties;
- Assessment of applicable sanctions laws;

- Appropriate screening of applicable sanctions lists, with proper calibration of automated programmes, and an appropriate amount of human involvement and an articulated policy for assessing and reporting possible matches;
- Training programmes, policies and procedures to report matches, licensing requests, and assess whether obligations arise under any other financial crime prevention laws; and
- Comprehensive but proportionate clauses in contracts.

There is no one-size-fits-all sanctions policy for financial institutions, but any programme should include at least these elements. It is also critical to have an overall financial crime compliance policy, to ensure the right matters are reported to the right authorities. For example, identifying a sanctions target that a firm must report to Treasury may (but will not necessarily) also cause the firm to form a suspicion of money laundering, which it may need to report to the National Crime Agency (NCA).

References

1. An example of this is the round of EU and US sanctions imposed on Russia in response to the Ukraine crisis. See 'Latest US/EU sanctions puts Russian energy exploration and lending in deep freeze', *TFR*, September 2014, at: www.tfreview.com/node/10911.
2. See: www.gov.uk/government/collections/financial-sanctions-regime-specific-consolidated-lists-and-releases.
3. See: www.gov.uk/government/publications/financial-sanctions-consolidated-list-of-targets.
4. HM Treasury issued general guidance for exporters following the 12 September sanctions here: www.gov.uk/government/news/doing-business-in-russia-and-ukraine-sanctions-latest.
5. The resource centre, which includes tools to search OFAC Specially Designated Nationals, Blocked Persons, and Sanctions lists, can be found at: www.treasury.gov/resource-center/sanctions/Pages/default.aspx.
6. An example of the ECO's guidance on Russian sanctions can be found at: http://blogs.bis.gov.uk/exportcontrol/uncategorized/notice-to-exporters-201422-new-eu-sanctions-against-russia/.
7. One example being the US$8.97bn fine imposed on BNP Paribas in respect of Sudanese oil finance in July 2014.
8. See: www.jmlsg.org.uk/.
9. See: http://fshandbook.info/FS/html/FCA/FC.
10. See: www.fca.org.uk/about/what/protecting/financial-crime. This is the FCA's 'Fighting financial crime' which contains links through to the thematic reviews

(including the one the FCA did on trade finance) and the 'Guide for firms' on financial crime.

11. For the FCA's current position on KYC see 'FCA financial crime risks final guidance softens KYC position', *TFR*, July 2014, at: www.tfreview.com/node/10660.
12. Published in August 2014 at www.iccwbo.org/Advocacy-Codes-and-Rules/Document-centre/2014/Guidance-Paper-on-the-use-of-Sanctions-Clauses-2014/.