Financial Conduct Authority

Thematic Review TR13/3

Banks' control of financial crime risks in trade finance

July 2013

This report contains new examples of good and poor practice. Please see GC13/3 for our consultation on the proposed new guidance.
Please note that we are not consulting on the findings in this report.

Contents

1. Executive summary

1.1 Introduction

1. This report describes how banks in the UK control money laundering, terrorist financing and sanctions risks (collectively 'financial crime risks') in trade finance business and sets out the findings from our recent thematic review.

2. Trade finance is a key component in maintaining a competitive and productive economy. London's position as a major financial centre could be severely affected if banks engaging in trade finance activity do not have appropriate systems and controls to prevent money laundering, terrorist financing and sanctions breaches from taking place.

3. We expect banks and other firms engaged in trade finance business to consider our findings and examples of good and poor practice and to use them to develop more effective policies and controls where necessary.

4. We will include these examples of good and poor practice in our regulatory guidance, to *Financial Crime: A Guide for Firms*. If you have any comments on the proposed examples of good and poor practice in this report, please respond to our consultation.

1.2 Findings

5. We found that banks had generally developed effective controls to ensure they were not dealing with sanctioned individuals and entities. However, policies, procedures and controls to counter money laundering risk were generally weak and most banks had inadequate systems and controls over dual-use goods.[1]

6. There were some exceptions where banks demonstrated a well-considered approach, but there was significant room for improvement at most banks.

7. Common weaknesses identified included the following:

   a. There was an inconsistent approach to risk assessment and only a few banks had conducted a specific trade finance money laundering risk assessment. With the exception of dual-use goods, banks generally had a more sophisticated, mature and better defined approach to managing the risk of sanctions breaches than to managing money laundering risk.

1 Dual-use goods include software, technology, documents, diagrams and other goods that can be used for civil and military purposes.

b. About half of the banks had no clear policy or procedures document for dealing with trade-based money laundering risks. As a result, some banks failed to implement adequate controls to identify potentially suspicious transactions.

c. Many banks were unable to demonstrate that money laundering risk had been taken into account when processing particular transactions. In particular, trade processing staff in most banks made inadequate use of customer due diligence information gathered by relationship managers or trade sales teams. However, a minority of banks used some innovative and effective techniques to assess money laundering risk in trade finance transactions, which other banks could usefully follow.

d. Most banks produced little or no management information on financial crime risks in the trade finance business.

e. Many banks, particularly smaller banks, had not developed specific trade finance financial crime training for relevant staff. As a result, we found evidence of staff failing either to make appropriate enquiries about financial crime risks or to escalate potentially suspicious transactions. Many banks relied heavily on the fact that trade processing staff were generally very experienced, but we often found they were not considering money laundering risk in practice. In addition, we found a poor understanding of trade finance money laundering risks among some MLROs and compliance staff with important AML responsibilities.

f. There was limited evidence that banks were escalating potentially suspicious transactions for further review and more senior level sign-off on the basis of money laundering concerns. Transactions were usually escalated for sanctions reasons or because the value of the transaction had exceeded a pre-determined threshold.

g. Systems and controls over dual-use goods were inadequate at most banks.

h. With the exception of one bank, our review did not identify any significant concerns with the general approach taken by banks to ensure they were not dealing with sanctioned individuals and entities. However, some banks need to do more work to assess whether staff are exercising the right judgements when closing down sanctions alerts, and others need to ensure that all entities involved in a transaction are appropriately screened.

1.3 Conclusions

8. Our main conclusion is that the majority of banks in our sample, including a number of major UK banks, are not taking adequate measures to mitigate the risk of money laundering and terrorist financing in their trade finance business. There were some notable exceptions to this, particularly among some of the larger US banks in our sample.

9. Most banks need to conduct significant work to ensure that all financial crime risks are routinely considered when processing transactions. In particular, staff responsible for managing financial crime risks required better training to identify potentially suspicious transactions.

10. More work is required at most banks to ensure high-risk customers and transactions are identified and appropriate action is taken by senior management. In addition, banks generally need to improve management information so that senior management are aware of how financial crime risks are evolving in this type of business.

11. Where banks fell short of our regulatory requirements, we have highlighted the areas where they need to improve. We are also considering where further regulatory action may be required for certain banks in our review.

2. Introduction

2.1 Objectives

12. This report is the result of a thematic review to examine how banks financing or facilitating international trade mitigate financial crime risks. The main purpose of the review was to assess anti-money laundering (AML), anti-terrorist financing (ATF) and sanctions controls in a number of banks and to measure the potential impact of financial crime on the trade system.

2.2 Background

13. 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 as one of the ways criminal organisations and terrorist financiers 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 organisations to transfer value across borders.

14. 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 become more attractive to criminals to use trade finance products.

15. Trade finance is a key component in maintaining a competitive and productive economy. London's position as a major financial centre could be severely affected if banks engaging in trade finance activity do not have appropriate systems and controls to prevent money laundering, terrorist financing and sanctions breaches from taking place.

16. This report summarises the findings of our review. It contains examples of good and poor practice that we identified, which we propose to confirm as formal FCA guidance following consultation.

2.3 Methodology

17. We aligned our review with the scope of the Wolfsberg Trade Finance Principles and looked specifically at the mechanisms used to finance the movement of goods and services across borders. Our focus was on Documentary Letters of Credit (LCs) and Documentary Bills for Collection (BCs), where trade-related documents (invoices, bills of lading, etc) are routed through banks and examined for consistency within the terms of a trade transaction.

18. We visited 17 banks in the UK between September 2012 and February 2013. This included four major UK banks, five global wholesale and investment banks and a number of smaller overseas

banks based in London. In April 2013, we conducted an overseas visit to examine offshore back-office trade finance processes at three major banks.

19. We chose our sample to ensure a good spread of banks by size. Each of the banks carried out trade finance business in countries and sectors, or with clients, which exposed them to higher levels of AML, ATF and sanctions risk.

20. None of the banks was selected because of pre-existing concerns about financial crime systems and controls in their trade finance business. So we consider our sample to be broadly representative of banks carrying on trade finance activities in the UK.

21. Before our visits, we consulted a range of stakeholders, including representatives from the British Bankers Association, the International Maritime Bureau, major consultancy firms and industry experts working in banks that were not part of our sample.

22. We requested information from all banks before visiting them, including relevant policies and procedures, risk assessments and training material. We also obtained details of trade finance payments linked to countries or sectors, or with clients, which exposed them to higher levels of money laundering, terrorist financing and sanctions risk.

23. We interviewed staff in key roles to understand the approach banks take to identify, assess and manage the financial crime risks in their trade finance business. These included staff from the business, compliance and operations areas, such as relationship managers (RMs) for trade finance customers, trade financing processing staff, specialist trade finance advisers and a range of risk and compliance personnel.

24. We reviewed the following areas:

- governance and management information
- risk assessment
- policies and procedures
- due diligence
- training and awareness
- money laundering controls
- terrorist financing controls, and
- sanctions controls.

25. We would like to thank the banks that participated in the review and the stakeholders for their advice and assistance.

2.4 Banks' legal and regulatory responsibilities

26. A range of laws, regulations, guidance notes and industry customs and practices are relevant to how banks design controls for countering money laundering, terrorist financing and sanctions breaches in trade finance.

27. The Money Laundering Regulations 2007 and Proceeds of Crime Act 2002 require firms to, for example, perform due diligence checks on their customers and report knowledge or suspicion of money laundering to the relevant authorities.

28. There are also regulatory requirements: the FCA's Handbook of Rules and Guidance requires, among other things, that banks establish and maintain effective systems and controls to prevent the risk that they might be used to further financial crime. Our document, *Financial Crime: A Guide for Firms* sets out examples of good and poor practice in how banks handle risks related to money laundering, weapons proliferation and sanctions compliance. However, neither the guide nor our Handbook covers trade finance specifically.

29. Several bodies have prepared guidance on the steps banks can take to tackle financial crime risks in trade finance. Guidance produced by the JMLSG and the Wolfsberg Group were frequently mentioned by banks during our visits. So were the UCP 600 and UCP 522 documents published by the International Chamber of Commerce (ICC). These ICC publications set out internationally-recognised customs and practice in relation to LCs and BCs, but do not cover matters related to financial crime.

30. Some banks highlighted that legal and regulatory requirements related to financial crime might conflict with the commercial obligations set out by the ICC. For example, if a bank took steps to counter financial crime risk that led it to fail to meet its commercial commitments, commercial litigation could follow. While some banks found this prospect unsettling, others felt the prospect of successful litigation against them in these circumstances was remote as their regulatory obligations and duties under criminal law would take precedence. This risk therefore appeared to be hypothetical, and no bank in our sample could provide an example of when this conflict had arisen in practice.

3. Findings

3.1 Governance and management information

3.1.1 Organisational structure

31. Our review considered banks' governance arrangements to oversee the management of financial crime risks in trade finance activity. We examined the role of management, escalation arrangements, information flows and organisational structure.

32. All banks had a range of staff in different areas contributing to the execution of trade finance transactions. There were various models for how this was structured, influenced by factors such as the geographical spread of business, the scale of operations and how trade finance fitted with a bank's wider menu of products. There were several key players in each institution.

Compliance staff – Compliance staff carried out a range of roles, often including AML and sanctions responsibilities. Some banks had dedicated trade finance compliance staff, in others the compliance brief covered a range of business lines and countries. Some compliance units had specialist staff offering technical advice on topics like trade embargoes and financial sanctions and performing extra due diligence on transactions (such as vessel searches[2] and checks to verify that the prices of goods on trade invoices were reasonable). In some cases their role included liaising with bodies like the Treasury's Asset Freezing Unit and the UK's Export Control Organisation. Some compliance staff provided staff training and maintained policies and procedures, and some also performed quality assurance checks by reviewing a sample of trade finance transactions after the event.

Trade processing staff – Most banks said staff processing trade finance transactions (from when documents are first received to when payments are made) are an important defence against financial crime. Their roles ranged from detecting potentially fictitious documents to spotting 'red flags'. Several banks suggested trade processing staff exercise an important control at the point they accept new Letter of Credit business, with potentially risky business filtered out at this stage. Some banks encouraged operations staff to perform checks, such as vessel searches, on their own initiative. At some banks the roles and responsibilities of trade processing staff were unclear. More generally, some banks' trade processing teams did not use the relationship managers' knowledge about their customers.

Relationship managers – Several banks suggested relationship managers dealing with clients were another important defence against financial crime risks. However at many banks, relationship managers we spoke with were focused on credit and operational risks and had limited awareness of trade specific financial crime risks.

At one bank, the relationship managers and trade operations staff felt it was the others' responsibility to identify high-risk customers and transactions. In practice neither was doing so.

2 It is possible to verify the details of a particular ship or shipment route using third party data sources accessible via the internet.

Audit – Some banks had conducted internal and/or external audit reviews of trade finance business in recent years. However, there were very few examples of financial crime controls over trade finance coming under specific scrutiny.

33. Effective communication between these functions is clearly important in managing financial crime risk. Some banks emphasised the importance of an open culture where questions about customers or transactions would be dealt with constructively.

> One global investment bank with trade finance operations across the world held monthly teleconferences, where different offices would discuss transactions that had been escalated (for reasons including financial crime concerns) to try to identify trends and spread knowledge of 'red flags'.

34. In some banks, we found evidence of dialogue between trade processing staff, relationship managers and compliance staff, although this was sporadic and usually related to sanctions issues rather than money laundering risk.

3.1.2 Escalation and the role of senior management

35. Although many larger banks said the role of senior management in relation to financial crime in trade finance was to set the right tone and demonstrate leadership more generally, we found limited evidence of transactions being escalated because of money laundering concerns. Where transactions had been escalated, this was usually because of a more general reputational concern (eg, it related to the export of defence equipment) or sanctions risk.

> One large bank referred a deal to finance the import of coastguard vessels to its reputational risk committee for that region of the world. Although the financial aspects of the deal appeared sound, the dual-use nature of the boats raised concerns and the transaction was turned down.

36. Some smaller banks focused on trade finance as a key business line and senior management therefore took a close interest and were able to demonstrate that the Money Laundering Reporting Officer (MLRO) was involved in decision-making related to individual transactions.

37. Some banks had committees in place that considered financial crime risks in trade finance as part of their remit. Several had global or regional reputational risk or transaction review committees that could consider trade finance transactions if a decision were necessary.

> Two large investment banks held regular forums to consider money laundering risk in trade finance business. One of these involved risk teams, compliance staff, legal counsel and business heads from different regions. It received reports on trade activity in higher-risk jurisdictions and industries to gauge whether AML risks in the portfolio of transactions were increasing.

3.1.3 Management information

38. We expect banks to develop regular reporting to senior management that gives senior management a useful view of how financial crime risks are evolving in its trade finance business.

39. Most banks produced little management information specifically on financial crime risks in trade finance. However, we did see some examples of statistical data covering, eg, completion rates for training courses and volumes of potential sanctions hits or escalations of suspect activity by staff. We also saw issues logs that recorded the bank's progress in addressing crystallised risks.

One bank reported aggregated data on sanctions alerts and AML alerts on a quarterly basis at a country, regional and global and product level. This helped the bank ensure that patterns or concentrations of unusual activity, potential training needs and procedural changes were identified.

Another prepared a monthly report to trade finance management covering compliance matters, including the volume of referrals of potentially suspicious activity. This pack informed the bank's recorded assessment of risk in the trade finance business.

3.1.4 Governance and management information – good and poor practice

Good practice

- Roles and responsibilities for managing financial crime risks in trade finance are clear and documented.

Poor practice

- There is a failure to produce management information on financial crime risk in trade finance.
- There is a lack of internal audit focus on financial crime controls in trade finance.
- The structure and culture of banks do not encourage the sharing of information relevant to managing financial crime risk in trade finance.
- There is failure to establish appropriate forums to allow knowledge and information sharing about financial crime risk

3.2 Risk assessment

3.2.1 What are the financial crime risks in trade finance?

40. The FATF, Wolfsberg and JMLSG have broadly categorised the financial crime risks in trade finance as money laundering/terrorist financing (including fraud), and sanctions/proliferation financing.

Money laundering/terrorist financing

41. Trade finance can be used to hide the illegal movement of funds or value – typically by misrepresenting the price, quality or quantity of goods, or even faking the existence of goods – and is dependent on some form of collusion between buyer and seller. There are a number of techniques for doing this:

a. over/under invoicing to misrepresent the price of the goods

b. short/over shipping to misrepresent the quantity or quality of the goods, and

c. so-called 'phantom shipping' where all documentation is completely falsified and there is no shipment of goods at all.

Sanctions/proliferation financing

42. There are a variety of United Nations, regional and national sanctions regimes in place. These regimes are broadly divided into: financial sanctions that target named individuals and entities; and trade-based sanctions that put embargoes on the provision of certain goods, services or expertise to specific countries. More recently, a number of UN Security Council resolutions have introduced activity-based financial prohibitions for certain countries, related to preventing the proliferation of weapons of mass destruction (WMD).

43. We found that all the banks we visited recognised the range of financial crime risks they faced in trade finance, albeit with varying degrees of emphasis, risk ratings and application of controls. A common view was that, historically, the main risk in trade finance was fraud, but now the financial crime risk profile had changed to sanctions, money laundering and WMD. In particular, banks were well aware of the threat to their business and reputation from committing breaches of sanctions, which could endanger their ability to clear payments.

> The MLRO of one major bank saw sanctions breaches as the biggest risk to his bank's business and disagreed with FATF's view that trade-based money laundering was increasing and that trade finance was a high-risk product for money laundering. This view was shared by the UK head of compliance, although he accepted that money laundering was an 'emerging area of risk' for the bank.

3.2.2 Banks' approach to risk assessment

44. We expect banks to adopt a risk-based approach to their assessment and management of financial crime risk in relation to trade finance, in the same way as with their other lines of business, services and products. But that approach, and the application of an appropriate control framework, must be tailored to the role of the bank in a particular trade transaction.

45. We found an inconsistent approach to risk assessment. While a few banks had conducted a discrete trade finance AML risk assessment, and kept it up-to-date, others had not. And we found that banks tended to have a more sophisticated, and better articulated, approach to managing the risk of sanctions breaches than to managing money laundering risk.

> One major US bank produced a Trade Services AML Risk Assessment document, which was updated annually.
>
> The document provided a comprehensive overview of: the bank's trade finance business; the AML and sanctions risks involved; the bank's exposure to those risks; and the controls around them. Various appendices to the document provided a wealth of useful additional information, including a long list of Trade Services 'red flags', annotated to show what certain red flags might indicate.
>
> This document had also proved to be a useful tool for educating senior managers about the technicalities of trade finance.

46. Apart from the US banks, which have a legal obligation to produce a documented AML risk assessment, we found that practice varied among the larger banks.

47. One European bank had an AML risk assessment manual, updated annually and covering the full range of products offered by the bank, including trade finance products. Two other banks followed a broadly similar approach to each other, carrying out a wider financial crime risk assessment either as part of an overall assessment of compliance risk or product risk. Another major UK bank completed an annual AML and sanctions risk assessment at business unit level to evaluate the inherent risk of that unit's portfolio and the effectiveness of controls in place to mitigate that risk.

48. At the other extreme, however, one major bank had performed no relevant assessment since a one-off exercise in 2009 to review financial crime controls in trade finance, identify gaps and recommend enhancements to procedures.

> One small foreign bank told us that trade finance was covered in its risk assessment of products and services included within the bank's AML handbook. However, we saw that the relevant extract was largely copied and pasted from the JMLSG guidance from 2011 and contained little more, by way of assessment or conclusion, than 'effective CDD procedures are needed' on its customers, which would include 'verifying their identities, nature of business and source of funding'.

49. The majority of smaller foreign banks had undertaken no financial crime risk assessment at all, in a couple of cases admitting that their focus was predominantly on credit risk. But there were some exceptions.

3.2.3 Mitigating and controlling risks

50. We found that, where banks rated trade finance as inherently high-risk business, the overall net risk rating was usually reduced – to medium risk or occasionally lower – by effective internal controls, such as comprehensive global and regional anti-financial crime policies and procedures, trade-based AML and sanctions guidance and knowledgeable and well-qualified staff. Furthermore, banks generally acknowledged that the risk varied according to the bank's role in a particular letter of credit or bill for collection (This is discussed in more detail in section 3.4 of the report.)

51. Where banks were issuing LCs, it was invariably the case that they would only do so for existing, well established, customers who were either large corporates whose business the banks knew well, or they were stock exchange listed companies. In such cases, credit limits were applied for LC issuance, which required appropriate due diligence to be performed. Similarly, where banks were negotiating or confirming LCs issued by their correspondent banks abroad, and thereby providing finance to the beneficiary of the LC, it was considered important to have a good knowledge and understanding of a particular correspondent bank's customer base and the effectiveness of that correspondent bank's own anti-financial crime control framework.

> Many banks told us that to 'retain the right clients' was a key control.

52. All the banks we visited placed a great deal of emphasis on the importance of having well trained and experienced trade processing staff. Because such transactions were largely paper-based, and automated transaction monitoring to pick up potential AML 'red flags' was very difficult, banks were heavily reliant on the judgement of staff to decide whether and when to escalate a transaction to a higher authority or the compliance team. If a staff member became suspicious of money laundering, they could also use certain tools, such as International Maritime Bureau (IMB) checks.

53. We found that sanctions controls could be better applied at two stages. Firstly, sanctions screening of all fields in a SWIFT 700 series message could take place at various stages in the life of an LC. And secondly, banks could typically screen all their incoming and outgoing payments for sanctions purposes, using a number of different proprietary software solutions.

3.2.4 Risk assessment – good and poor practice

Good practice

- Completing a documented financial crime risk assessment for trade finance business that gives appropriate weight to money laundering risk, as well as sanctions risk.

Poor practice

- Failing to update risk assessments and keep them under regular review to take account of emerging risks in trade finance.
- Only focusing on credit and reputational risk in trade finance rather than carrying out a proper consideration of financial crime risk.
- Not taking account of a customers' use of the bank's trade finance products and services in a financial crime risk assessment.

3.3 Policies and procedures

54. Once banks have identified and assessed the financial crime risks in their trade finance business, they must ensure that appropriate policies and procedures are in place to manage those risks. They should enable banks to identify trade finance customers and transactions that pose the highest financial crime risk, and set out well-defined processes with clear lines of responsibility for assessing and mitigating risks. The nature of trade finance business should allow banks to consider financial crime risks at various stages of a transaction, including whether or not a transaction presents an unacceptable financial crime risk.

55. Policies and procedures should be regularly updated to take account of emerging risks and should have the full support of senior management. They should also be readily accessible, effective and understood by all relevant staff. In recent years, bodies such as the FATF and Wolfsberg Group have issued guidance on the steps bank can take to identify and prevent financial crime risks in their trade business and we would expect a bank's policies and procedures to reflect this guidance.

56. Although most banks did not have a stand-alone trade finance AML or sanctions policy, procedures and controls tended to conform to the overarching requirements of a bank's main AML and sanctions policies.

> A major UK bank's MLRO told us that 'we take group policy and, through implementing policies and procedures, turn it into something more real'. There was no discrete trade finance policy. Trade finance was referenced in AML and sanctions policies and procedures.

57. Some larger banks had implemented effective procedures to tackle financial crime risks in their trade finance business. However, we were concerned that the majority of banks had no clear policies or procedures for staff to follow when assessing money laundering or terrorist financing risks in trade finance. Many of these banks were unable to provide us with evidence that relevant staff had considered money laundering risks in high-risk transactions and there was often limited evidence that escalations had been made, despite there sometimes being good reason to have done so. In particular, policies and procedures were not usually AML-specific and focused on credit and operations aspects of a transaction.

One bank told us that they did not have a stand-alone trade finance AML policy, but that trade finance was included within the Group AML policy, along with other relevant topics such as sanctions policy, guidance in relation to high-risk countries and instructions for conducting AML risk assessments. However, we found the specific guidance on trade finance in the policy was very limited. As a result there were very few controls in place to identify high-risk transactions and there had been very few escalations made by relevant staff, except on the basis of sanctions risk.

58. Weak policies and procedures sometimes meant that responsibility was not always clear. We had a number of meetings where relevant staff in one part of a bank felt that it was another area's responsibility to identify and assess the financial crime risks. The consequence was that neither part of the business was taking ownership of identifying high-risk transactions.

59. Generally we found banks had more developed and robust policies and procedures for dealing with sanctions risks in their trade finance business. This is, in part, explained by the fact that many banks told us they considered sanctions to be the main financial crime risk when processing trade finance business. Sanctions policies tended to be more detailed and prescriptive, enabling staff to more closely follow a process when assessing these risks.

One bank had a document setting out guidelines for sanctions due diligence and identifying and managing the escalation of sanctions hits in its trade business. Another bank had a Special Risk Client Policy, which restricted the types of business this bank could undertake with certain entities.

60. Some banks required compliance checks for products that were perceived to be higher risk, such as Export LCs. Yet these checks did not always include AML considerations and were often focused on sanctions issues, such as embargoes on dual use goods.

61. Some banks had procedures to check that transactions were in line with the known previous activity of a customer. At some banks, staff were required to consider the countries and goods associated with transactions and, where they corresponded with banks' high-risk countries or goods lists, they may be referred to the legal and/or compliance departments.

An overseas bank had a detailed description of high-risk goods that might trigger a referral to the compliance department. Goods were classified into four main categories: nuclear, chemical, biological and missile/delivery. These goods descriptions were intended only as a guide for staff and the MLRO expected concerns to be raised even if the description of the goods did not completely match.

62. Most banks had detailed sanctions screening guidance in place. One bank's guidance included a requirement to screen ports, storage houses, inspection companies, insurance companies, and any individuals connected with them. The guidance stated that, where details were not contained within the SWIFT messages, they must be screened manually. However, other banks were not routinely screening information in trade documents. Banks should review their procedures and ensure they include a requirement to screen all relevant parties to a transaction.

63. Many banks had specific policies for weapons, military and defence goods, which often required staff to escalate for approval.

At one bank, we were told that if a foreign army was importing shower gel, that transaction would require escalation, regardless of the amount. The transaction would need to be signed off by the managing director and the Reputational Risk Committee. In every case, the bank had to be sure who the end-user was.

Good practice in a small bank

64. A small overseas bank was ahead of its peers in providing a discrete trade finance section within its AML manual. It was based on the FATF's 2006 study of trade-based money laundering[3] and highlighted the money laundering and terrorist financing risks for staff to be aware of in trade finance business. The manual instructed staff to consider the parties involved in a transaction and the countries where they were based, as well as the nature of any goods in the underlying commercial transaction. It also listed 12 'red flag indicators' set out in the FATF report, which might be indicative of trade-based money laundering.

65. Clearly defined procedures specified that appropriate and acceptable due diligence must be carried out on the instructing party for the transaction, as well as other parties in certain circumstances. The procedures made it clear who should be deemed the instructing party for import and export LCs and inward and outward BCs.

66. There was also a specific section that listed some of the additional measures that might be considered appropriate when carrying out enhanced due diligence for particular transactions. These measures included: further enquiries on the ownership and background of the instructing party or the beneficiary; building up a record of the pattern of an instructing party's business; using the services of the ICC's International Maritime Bureau (for warning notices) and Commercial Crime Services (for bills of lading, shipping and pricing checks); and holding relationship meetings and/or conducting visits to instructing parties.

3.3.1 Policies and procedures – good and poor practice

Good practice

- Staff are required to consider financial crime risks specific to trade finance transactions and identify the customers and transactions that present the highest risk at various stages of a transaction.
- Staff are required to screen all relevant parties to a transaction.

Poor practice

- Very little money laundering guidance on financial crime risks specific to trade finance.
- Staff are not required to consider trade specific money laundering risks (eg, FATF/Wolfsberg red flags).
- Procedures do not take account of money laundering risks and are focused on credit and operational risks.
- No clear escalation procedures for high-risk transactions.
- Procedures fail to take account of the parties involved in a transaction, the countries where they are based and the nature of goods involved.

3 www.fincen.gov/news_room/rp/files/fatf_typologies.pdf

3.4 Due diligence

3.4.1 General

67. We expect banks, in line with JMLSG guidance, to conduct sufficient and appropriate due diligence on the relevant parties to a trade finance transaction, adopting a risk-based approach that takes account of the bank's particular role in LCs or BCs.

3.4.2 What does the JMLSG advise?

68. The JMLSG guidance states that, with the partial exception of BCs, due diligence must be carried out on the customer who is the 'instructing party' for the purpose of a particular trade finance transaction.

69. Due diligence on other parties to the transaction, including other customers, should be carried out where required by a bank's risk policy. Additional due diligence on other parties, and possibly on the transaction itself, should be undertaken where required by the bank's internal risk policy and where the bank is specifically 'on enquiry'.

70. The instructing party will normally be an existing customer of the bank but, if not, due diligence must be carried out on the instructing party before proceeding with the transaction.

3.4.3 Who is the instructing party?

71. For import LCs, the instructing party for the issuing bank is the applicant. So where LC facilities are required, the issuing bank should seek information from the applicant about: countries in relation to which the applicant trades; trading routes used; goods traded; the type and nature of parties with whom the applicant does business (eg, customers, suppliers, etc); and the role and location of agents and other third parties used by the applicant in the course of its business.

72. For export LCs, the instructing party for the advising/confirming bank is the issuing bank. The advising/confirming bank should carry out appropriate due diligence on the issuing bank in line with relevant JMLSG guidance on correspondent banking, which will entail regular reviews of the correspondent banking relationship. Consequently, due diligence on the issuing bank need not be performed each time an LC is received by the advising/confirming bank.

73. Although there is no requirement to carry out customer due diligence on the beneficiary of the LC, the JMLSG guidance suggests that it may be appropriate to perform some basic checks. These may comprise checking: the existence of the company at Companies House (or equivalent foreign registry); online trade directories, professional advisers or financial statements that might help to confirm the validity of the transaction; and the goods, shipment routes or payment terms if the LC has been issued by a bank in a high-risk country.

74. For export BCs, the instructing party is the customer/applicant. The JMLSG guidance notes that normally the instructing party (exporter) will already be the bank's customer, on whom due diligence has already been performed.

75. For import BCs, due diligence should be carried out on the drawee[4], who will normally be the importer or an agent of the importer. As with export BCs, the drawee is typically an existing customer of the bank receiving the collection, so standard anti-money laundering due diligence should already have been carried out. But the JMLSG guidance adds that further enquiry by the bank may be justified, depending on the nature of the transaction and whether it appears consistent with the scale and nature of the customer's known trading activity.

4 Drawee is an entity/person upon whom a bill of exchange is drawn and who is thereby ordered to pay.

3.4.4 Findings

76. We found that, without exception, banks would only issue LCs for existing customers, on whom due diligence had already been performed. Typically, for both larger and smaller banks, that due diligence was carried out by a specialist know your customer/customer on-boarding team who operated completely separately from the teams processing trade finance transactions. However, practice varied on whether the on-boarding procedure incorporated discrete trade finance elements or whether, once on-boarded, the customer was permitted to undertake any kind of business with the bank.

> A major bank risk assessed new customers for anti-money laundering purposes, with the risk rating determining the level of due diligence performed and the frequency of subsequent reviews. However, the products a customer wanted to use were not factored into the risk assessment. This meant that using the bank's trade finance services did not increase the customer's risk rating, despite trade finance being considered by the bank to be a high-risk product.

77. Larger banks tended to operate a single customer on-boarding system, which incorporated various levels of customer due diligence (CDD) and held all the bank's CDD records. Different risk factors, eg, a connection with a high-risk jurisdiction or the customer being regulated by an approved regulator or exchange, could push CDD requirements up or down a level and product-specific risk factors, such as involvement in trade finance, were also taken into account.

78. Where enhanced due diligence (EDD) was required by a bank's AML policies and procedures, gathering the additional EDD data, analysis of any connections to politically exposed persons (PEPs) and the results of adverse media checks often led to discussions between a number of different teams (sales, product, compliance, etc) before the requisite senior management sign-offs could be obtained and a decision reached.

> One large bank told us that, because trade finance was deemed high risk, product due diligence was required for trade. So, in addition to performing the necessary CDD, it used a specific questionnaire for corporate clients who wished the bank to issue LCs and do documentary collections. Accordingly, sales staff were required to gather a lot of relevant information, including: who the client's suppliers were; what goods the client purchased; from where; and expected volumes and values for LCs and BCs. The questionnaire was used for both one-off requests to issue a LC and a facility to issue LCs up to a certain limit.

79. At smaller banks, normal CDD procedures usually captured sufficient information about the customers' business and where it took place. Often, these banks had a base of long-standing trade customers who did a lot of repeat business, which was well known to the banks. But where, for example, a customer only occasionally wanted to do a trade finance transaction, they would be asked to complete a trade finance information form.

One small foreign bank had a specific section on trade finance in an appendix to its know your customer standards document. This included a table setting out CDD requirements, depending on which part of the trade transaction the bank was facilitating. A section entitled 'trade finance enhanced due diligence' covered what should be considered where a trade transaction displayed higher-risk characteristics, including:

- On the export side, obtaining more information on all parties to the transaction, particularly the seller, and establishing country of residence and existence of the buyer.
- On the import side, seeking information from the instructing party about the frequency of trade and the quality of the business relationships existing between the parties to the transaction.
- Checking public source information for prices of goods such as commodities and carrying out further investigation where there was a significant difference from the market price.
- Attending and recording relationship meetings with the instructing party, eg, by visiting them.

80. We found a clear segregation of duties between know your customer teams and trade processing teams. In all cases, processing trade finance transactions could not begin unless complete, up to date CDD was in place for the client concerned. This meant that trade processing teams had no access to CDD information and had to refer to relationship managers with any queries they might have. In general, trade operations team members had no more than a broad awareness of size and type of expected trade transactions and would escalate anything that fell outside that. However, at some banks, it was clear that information sharing between relationship managers and trade operations team members was not working effectively.

81. We found that all banks, large and small, treated the issuing bank as their Financial Institution (FI) client when advising or confirming an LC. It was, therefore, important to ensure that full, up to date CDD information was held on the issuing bank before processing an LC received for advice and/or confirmation. But practice varied between banks on whether CDD needed to be performed on non-client beneficiaries of LCs received.

One large bank took the view that if it had know your customer information on the issuing bank, there was no need to perform checks on the beneficiary unless it was confirming the LC and incurring credit risk.

In contrast, another large bank considered that some due diligence was required on non-client beneficiaries, even if the LC was merely being advised. In these circumstances, the advising bank would undertake some, or all, of the following: Google check; Companies House check; and/or review the beneficiary's website (where possible) to check that its line of business matched the trade transaction. If, after conducting these checks, the advising bank was still not satisfied, it might seek to arrange a meeting with the beneficiary company to obtain further information.

82. Smaller banks, with one exception, only conducted basic PEP and sanctions checks on non-client beneficiaries. One small foreign bank, however, when processing an export LC, would either update any missing details from the CDD it held on the issuing bank or, if necessary, perform full due diligence on the issuing bank before processing the transaction.

Group Introduction Certificates and dealing with other group entities

83. A number of banks in our sample were UK branches or subsidiaries of foreign banks, and we found that Group Introduction Certificates (GIC) might be a contentious issue.

84. One large American bank was adamant that it would not rely, in any circumstances, on CDD undertaken by other group entities and evidenced by a GIC. A large European bank had encountered problems where its FI relationships were managed by a head office team located overseas, who were responsible for gathering the necessary EDD on those FIs and providing a GIC to the UK bank. In a number of cases, the controls over the GIC process had failed, which

presented a significant degree of financial crime risk, given the volumes of export LC business handled by the UK bank. Consequently, the MLRO was about to initiate a GIC review.

85. There also appeared to be a risk of banks being complacent about money laundering risk in transactions where the counterparty FI was part of the same group – for example, where a bank advised an LC issued by their parent bank.

> One bank gave an example of a potentially suspicious transaction when an LC had been issued by their parent bank. The LC gave a Korean address for the beneficiary, but when the bank conducted an internet search on the address it appeared to be for a company registered in Nigeria.

3.4.5 Due diligence – good and poor practice

Good practice

- Banks' procedures are clear about what checks are necessary and in what circumstances for non-client beneficiaries (or recipients) of an LC or BC.

Poor practice

- Written procedures do not make it clear what due diligence must be carried out on the instructing parties to an LC or BC depending on the bank's role in a transaction.
- Trade processing teams do not make adequate use of the significant knowledge of customers' activity possessed by relationship managers or trade sales teams when considering the financial crime risk in particular transactions.
- Lack of appropriate dialogue between CDD teams and trade processing teams whenever potential financial crime issues arise from processing a trade finance transaction.

3.5 Training and awareness

3.5.1 Introduction

86. Good quality training is one of the most important tools that banks can use to prevent and detect financial crime risks occurring in trade finance business. In addition, the Money Laundering Regulations 2007 require firms to take appropriate measures so that all relevant staff are regularly given training in how to recognise and deal with transactions and other activities which may be related to money laundering or terrorist financing.

87. Relevant staff are likely to include relationship managers for customers engaged in trade finance activity, staff involved in selling trade finance products, and trade processing staff and control functions such as compliance, risk and internal audit. This list is not exhaustive and banks may identify other staff who fit into this category.

88. Bespoke training should be aligned with a bank's policies and procedures and should equip staff with the skills, knowledge and expertise to identify risks and take appropriate action – for example, escalating potentially suspicious transactions. Banks should regularly refresh their training to take account of emerging risks, to keep records of staff that have completed the training, and to ensure any issues in relation to gaps in staff knowledge are followed up.

3.5.2 Findings

89. Trade finance is a complex, specialist area where staff often have many years of experience. However, some banks were now finding it difficult to recruit staff with experience of trade finance.

> One MLRO said he had implemented a 'deliberate strategy' to hire staff with significant (20+ years) experience and was now planning more junior hires to whom this experience can be passed on.

90. A number of trade finance staff had passed a globally recognised professional qualification for international trade finance practitioners. However, this qualification did not cover, in any detail, the financial crime risks in trade finance business.

91. We were therefore concerned that, although all banks had generic money laundering/terrorist financing and sanctions training programmes, many banks had not delivered adequate training to relevant staff on the specific money laundering risks in trade finance. Many banks' trade-specific financial crime training was focused on sanctions risks, with limited coverage of money laundering. One bank's training material did not mention any of the FATF/Wolfsberg red flags. While it was encouraging to see that training on sanctions risks was generally well considered, we were disappointed that many banks had not placed an equivalent focus on money laundering and terrorist financing risks.

> At one bank, training included extensive details relating to the background of the sanctions regime, including an update to recent changes (e.g. some Libyan accounts being de-listed; relevant systems and processes, including escalation/approval procedures for sanctions alerts, and country-specific information – for example, there were eight pages dedicated to Iranian sanctions).

92. As a result, some trade processing staff did not have the knowledge or awareness to identify transactions that posed a high risk of money laundering and had not made appropriate enquiries to satisfy themselves about potential money laundering risks. In addition, staff outside trade processing teams were often unable to challenge the decisions taken by trade processing staff as they had a poor understanding of specific financial crime risks in trade finance.

> One bank used the specialist knowledge and experience of its trade finance staff when developing its training programme. This helped promote: awareness of the risks associated with particular commodities; checking rail consignment bills; and the challenges presented by truck shipments, among staff less familiar with these risks.

93. More positively, some larger banks had developed comprehensive training programmes tailored to consider the trade-specific financial crime risks. At one bank, staff received trade-specific online training covering AML risks, suspicious activity (including the FATF/Wolfsberg Red Flags list) and sanctions. The training had a strong practical dimension, with case studies showing staff how to handle high-risk transactions. The training had been regularly updated and was approved by the bank's Trade Services AML team.

One bank raised awareness of financial crime risks by asking staff to adhere to the '10 Trade Operations Commandments', which were:

- Know your customers
- Detect red flags
- Sanction screen every transaction
- Know goods involved in each transaction
- Know the end-use
- Know the end user
- Know the destination country
- Verify if licence is required
- Store documents/communications for records
- Escalate if in any doubt

Another bank had put together a series of questions to be considered as part of any transaction review. These included:

- What is the background of companies and are they related in any way?
- Is the transaction consistent with regular business activities?
- Is the transaction structure overly complex or unusual?
- Are high-risk commodities involved?
- Are high-risk countries involved?
- Are there any concerns regarding the quality and quantity of goods?
- Have any pressure tactics been applied by the customer?
- Is non-standard terminology used?
- Is the price consistent with the market?
- Are there any anomalies with the presented trade documents?

94. We found some issues in relation to the consistency of training for relevant staff in different locations. For example, a bank with relevant operations in the UK and India had offered a good level of face-to-face training to staff in the UK, but staff in the bank's Indian operation had not received an equivalent level of training since 2008.

Effective training techniques

95. We observed a number of simple and effective measures that some banks used to ensure staff engaged well with the training and awareness material provided. These included:

a. keeping training courses short and focused

b. delivering training via innovative means (eg, web and video based training and quizzes)

c. using real and relevant case studies, and

d. poster campaigns.

96. We found that banks using case studies of transactions that had been escalated were most effective in raising awareness among staff.

97. Many banks kept staff aware of current risks via relevant industry publications including the bi-monthly IMB bulletins and its black list of shipping issues and other publications such as

'Documentary Credit World', which includes useful information on prevailing LC practices, as well as a section on fraud and relevant litigation cases.

3.5.3 Training and awareness – good and poor practice

Good practice

- Providing tailored training that raises staff awareness and understanding of trade-specific money laundering, sanctions and terrorist financing risks.
- Using relevant industry publications to raise awareness of emerging risks.

Poor practice

- Only providing generic training that does not take account of trade-specific risks (eg FATF/ Wolfsberg red flags).
- Failing to roll out trade specific financial crime training to all relevant staff engaged in trade finance activity, wherever located.
- Relying on 'experienced' trade processing staff who have received no specific training on financial crime risk.

3.6 Anti-money laundering procedures

3.6.1 Introduction

98. We expect banks to have a framework in place to assess money laundering risks in trade finance transactions and to identify, escalate and scrutinise the transactions that present a higher risk.

99. However, anti-money laundering procedures at a number of banks were not well developed to identify unusual or higher risk specific transactions. This was usually because banks had either not perceived the money laundering risk to be significant or because they felt the risk was managed through other means (eg, through customer due diligence procedures – see Section 3.4).

> The MLRO at one bank told us that the risk of money laundering was 'nowhere near as high as people say it is'. At this bank, we found that systems and controls to detect money laundering were weak.

100. It was clear from our review that, at times, there can be a conflict between the commercial pressure to proceed with a transaction and a bank's duty to comply with relevant money laundering legislation and guidance. Although banks will not want to reject transactions unnecessarily, they should ensure that sufficient attention is given to possible trade-based money laundering and that trade processing teams are given time to fully investigate potentially suspicious activity.

> At one bank it appeared that where further investigation was undertaken, the main aim was to obtain evidence that could support the decision to continue processing.

3.6.2 Transactional anti-money laundering controls

101. In all banks, trade processing teams were responsible for scrutinising the detail of each transaction to ensure compliance with applicable terms and conditions – a process widely referred to as 'document checking'. These teams had access to the specific details of a transaction and were therefore well placed to identify potential financial crime risks, including money laundering.

102. However, the extent to which banks had developed AML procedures for staff to follow varied significantly. Seven banks did not require staff to consider money laundering risks when processing a transaction. And all but two of the other banks relied solely on brief attestations by trade processing staff that money laundering risk had been considered.

Banks must meet their legal and regulatory obligations in relation to the reduction of financial crime. Some banks told us they only 'deal in documents' and that they are under no obligation to investigate underlying trade transactions. Some banks referred to UCP600, which states that banks are only required to take documents 'on their face'. However, one bank included a disclaimer in all trade finance transactions that allowed it to exit a transaction if possible sanctions, money laundering or other regulatory breaches had been identified. This report contains guidance for banks on how they might meet their legal and regulatory obligations.

103. It is important to consider money laundering risk throughout the life of a transaction. There are a number of phases during a transaction where money laundering risk can be considered and transactions can be escalated where appropriate (eg, before the release of an MT700, on receipt of trade documents and before payment). Given the commercial pressures associated with processing transactions in a timely manner, it is good practice for banks to ensure staff escalate suspicions for investigation as soon as possible and not, for example, just before payment is to be made.

A UK-based beneficiary presented documents to a bank in relation to an export LC, which included a request for payment to be made to a bank account in Hong Kong. Until this point there had been no indication of a link to Hong Kong so the transaction was escalated by the payments team to a trade specialist team. This team undertook some further research and established that the beneficiary had a legitimate connection to Hong Kong and as a result the transaction was cleared to proceed.

3.6.3 Identifying higher-risk transactions

104. The approach banks took to identify money laundering risks in transactions varied across the sample. We found that banks considered a range of the following factors when reviewing transactions:

- The name and location of key counterparties, ports of loading and discharge, methods of transportation, the nature and pricing of goods, and whether or not any of these alone or in combination give rise to suspicion or do not make sense.
- Using publicly available and/or subscription-based third party sources to verify information about the transaction.
- Due diligence information about the customer including expected goods, usual countries dealt with, and common counterparties to help staff make informed judgements about transactions.

- Having two trade finance processors review a transaction independently of each other to ensure red flags are not overlooked.
- Periodic quality assurance of judgements made by trade processing staff.

One bank received an instruction to process an export LC for a commodity on behalf of a beneficiary based in the UK and an applicant based in central Africa. The port of discharge was in a country outside the UK, which was not known for the production of the commodity. In addition, the name of the applicant matched a name on the bank's internal watchlist as the applicant was known to have previously engaged in unusually complex commodity transactions, above market prices. The transaction was escalated to the compliance team who required the trade processor to investigate the price quoted in the LC and confirm this was in line with the prevailing market price; he also confirmed that the structure of the trade was not complex.

Further inquiries established that the certificate of origin showed that the goods had indeed been produced in the same country as the port of discharge. As a result the decision was made to proceed with the transaction.

105. At many banks, it was not always clear that trade processing staff would identify transactions that were potentially suspicious. This was because they often did not have access to underlying CDD information or receive appropriate guidance/training.

Some banks' processes for identifying potentially suspicious transactions were too informal. One MLRO told us 'I would imagine if something was out of character for a customer it would be noted'. Another bank told us that unusual transactions would 'stick out like a sore thumb' despite the fact there were inadequate processes in place.

106. We saw examples of transactions where it did not appear that trade processing staff had carried out additional checks and/or escalated transactions despite there being good reason to do so.

We examined one transaction where the applicant and the beneficiary appeared to be part of the same group of companies, one of the counterparties was based in the British Virgin Islands and the port of discharge was stated as being 'offshore'. However, this transaction had not been subject to additional checks or consideration and, when we challenged the bank about this, they did not accept that further enquiries might have been sensible.

107. Some banks told us that the risk of staff lacking the necessary experience and awareness of trade finance risks could be a particular issue when trade processing teams were based offshore. However, we carried out visits to three banks' overseas trade processing centres and found that two had implemented effective procedures for appropriately trained staff to follow, which ensured the adequate identification and escalation of high-risk transactions.

108. However, at the third bank's offshore operations, trade processing staff were not sufficiently aware of trade-based money laundering risks. The bank had developed a money laundering checklist to be used by staff when processing each transaction but they did not appear capable or authorised to consider any other factors that might cause concern.

At one bank, we examined a transaction where scrap metal (a high-risk commodity in money laundering terms) was being sold by a company in the British Virgin Islands to a company in Sharjah, UAE. The transport documents indicated that the scrap was to be transported overland from Sharjah to Dubai but there were no details of the party to whom it was being delivered. The bank did not appear to have carried out any further inquiries.

109. Some banks relied entirely on the training given to staff and had no formal processes for considering money laundering risk. As mentioned in Section 3.5, we found that most banks' training did not sufficiently cover money laundering risk in trade finance. Most of the banks that relied on training were unable to demonstrate that trade-based money laundering risks were being managed appropriately.

One bank relied on staff to remember red flags they had been shown during training. This created a risk that red flags were either forgotten or wrongly interpreted.

110. Relationship managers play a key role alongside trade processing staff in identifying potentially suspicious transactions. At some banks it was clear that relationship managers were involved in the process of identifying potential money laundering in transactions. However, at a number of banks, this was not the case. Many were unable to describe potential suspicions in relation to money laundering and focused heavily on credit risk. Furthermore, they did not appear to have access to sufficient detail about a transaction early enough in its lifecycle, to ensure that money laundering suspicions were identified and properly considered before payments were made.

One bank required a dual sign-off approach for each transaction, with one signatory the relationship manager and the other a member of the trade processing team. This helped ensure the bank used the relationship manager's knowledge of the customer alongside the trade processing team's expertise. The documentation from this process was evidence that money laundering risk had been considered.

Challenges

111. Wherever possible, banks should obtain copies of the underlying trade documentation for review. However, we found there were challenges for firms dealing in certain types of transactions, including:

a. Those where a bank is acting as the advising bank in an LC transaction – in these circumstances, the bank does not always receive the underlying trade documentation as the beneficiary may choose to send the underlying trade documentation directly to the issuing bank.

b. 'Direct' outward collections, where the exporter (who is often a long standing customer of the remitting bank) may send documents directly to the importer's (presenting) bank under the letter head of the remitting bank.

c. When financing is provided on the basis of an invoice and letter of indemnity. This is common practice in the oil industry, where a consignment may be bought and sold a number of times before shipment has occurred. Under these circumstances it is not practical for a bank to receive all the trade documents (ie, bill of lading) before making payment.

112. In these difficult circumstances, banks should ensure that sufficient scrutiny is applied to any information that is available, such as the SWIFT MT700 message.

3.6.4 Money laundering red flags

113. Where banks had procedures in place to identify high-risk transactions, the process usually included a requirement to consider certain 'red flags' that were often based on those identified by the FATF and Wolfsberg.

> At one bank a member of the processing team was not aware of any FATF or Wolfsberg red flags and could not provide his own examples of red flags, or examples of transactions that he had escalated on the basis of suspected money laundering.

114. We have included in Appendix 1, details of red flags that trade processing staff were considering and some common examples are listed below:

- Continuous container numbers on a bill of lading (as they are generally random).
- Unusual transaction size (given what is known about the goods/customer).
- A shipment route that does not make sense (eg, if a certain good is being shipped to a country that is known to be an exporter of that good, or a route that is not normally used).

> One bank cited an example of a credit issued by an Iraqi bank for a large shipment of sugar to Brazil. This was escalated due to the size of the transaction and the banks' suspicion regarding the unusual flow of goods (ie, sending sugar to Brazil) It turned out that the Iraqi bank knew nothing about the transaction, so it was declined.

- Complex transaction structures.
- The beneficiary and applicant appear to be group companies.
- Port descriptions such as 'any safe world port'.
- Addresses in offshore centres.

> One bank told us that 'offshore jurisdictions do not present a particular issue as the transaction is often covered by a letter of indemnity'. The presence of a letter of indemnity would not normally be considered a control against money laundering; it might even suggest that additional scrutiny should be applied. In contrast, another bank told us they would not enter into transactions structured with a letter of indemnity, and would consider this type of structure to be a red flag.

115. Nine banks had issued guidance for staff on red flags to look out for when processing transactions. For example, one bank's risk decision matrix for trade processing staff required staff to consider an extensive list of red flags, specific high-risk goods and high-risk jurisdictions. Where red flags are used by banks as part of operational procedures they should be regularly updated and accessible to staff. And, in addition to considering specific red flags that may be part of a bank's procedures or guidance, staff should also be aware of other forms of potentially suspicious activity that may arise.

One bank had a central list of money laundering red flags that was updated regularly by the compliance and trade processing staff. This list was made available as a desktop aide-memoire to every member of the trade processing team. Lists of high-risk countries and industries were also provided alongside the red flags. If two or more of the red flags/countries/industries were identified in a transaction, then it had to be escalated. It is important to note that escalations could still be made on the basis of suspicion even if there were no direct matches with the aide-memoire.

116. Even where banks did reference red flags in their procedures, we found that some banks placed too much emphasis on the value of a transaction when deciding whether or not to escalate potential suspicions and some only escalated higher value transactions. It is important that banks are aware of the money laundering risk in lower value transactions.

3.6.5 Record keeping

117. Evidence of anti-money laundering reviews was generally weak. Ten banks' procedures required specific money laundering checks, yet only two retained adequate evidence that they had been carried out. The remaining eight banks relied on sign-off by trade processing staff, either electronically or on a printed coversheet, without any other information.

At one bank, processors would simply enter 'AML done' onto the bank's processing system once they had completed their compliance checks. No evidence was kept to show the quality of the checks carried out, the rationale for decisions, or even whether or not the checks had in fact been carried out.

118. The seven banks whose procedures did not require specific money laundering checks unsurprisingly had no record that checks had been undertaken. In contrast, most banks retained copies of the trade documents presented for each transaction.

One bank said there was 'no requirement to sign off that the processor has considered AML' and that 'reporting by exception is the only way an AML consideration could be demonstrated'.

119. It is important that banks retain adequate records so they are able to demonstrate that controls are operating effectively. Banks that fail to do so will find it difficult to carry out effective compliance monitoring or quality assurance testing and will find it difficult to demonstrate to regulators that money laundering and other risks are being managed effectively.

One bank's transaction checklist required trade processing staff to consider the parties, countries and goods involved in the transaction and any higher risk factors (including any red flags). However, the checklist was 'tick box' in nature, with no evidence of consideration by trade processing staff of factors other than those on the checklist and no rationale recorded for decisions made. Some of the questions on the checklist – particularly around pricing – were often left blank. It appeared that transactions were referred to the compliance team mostly on the basis of country risk rather than trade-specific anti-money laundering red flags.

3.6.6 Escalations and suspicious activity reporting

120. We found that four banks had no procedures for escalating potentially suspicious trade finance transactions for further investigation. At the other banks, there was often limited evidence that procedures were being adhered to or that high-risk transactions were being identified and escalated on the basis of money laundering concerns.

The trade processing team at one bank told us that any doubts about a transaction would be referred to the relationship managers in the first instance – yet our subsequent interview with one of the relationship managers revealed that he rarely received queries from this team. At a major bank we were told that 'it [an escalation] just doesn't happen as there are only a small number of regular customers that we deal with', even though they dealt with roughly 1,200 customers.

121. This was surprising given the volume of transactions that some banks, particularly major banks, were processing. Where examples of escalated transactions were provided, they usually related to potential sanctions breaches or exceeded a particular monetary threshold.

122. However, there were notable exceptions where banks demonstrated that appropriate escalations had been made on the basis of money laundering concerns. For example:

a. One bank had a specialist team of trade advisers and fraud investigators who were responsible for carrying out a second-line review of transactions that had been escalated by the trade processing teams. They provided regulatory guidance in relation to money laundering, sanctions, high-risk goods (including dual-use goods) and export controls to processors. They also carried out further checks on LC transactions that had been escalated to them, including the verification of the applicant and beneficiary's line of business, pricing checks, and vessel checking and shipment tracking.

b. Another bank had adopted a two-stage escalation approach. The first review was conducted by trade processing staff who considered a set of money laundering red flags. If red flags were identified, they escalated the transaction to a team of process experts who would review the transaction in more detail. This team would complete an 'AML decision document', which recorded the red flags that had been identified, any relevant comments and a rationale for the final decision that was made. Supporting documentation was attached where necessary.

c. A transaction was declined at one bank where 'urea' was being purchased by a suspected shell company located at a PO Box address in the Isle of Man. The opaque company structure of one of the main counterparties and the fact that the shipment involved urea – which is attractive to money launderers as it can fluctuate significantly in value, making bogus prices difficult to detect – was sufficient to raise suspicion at the bank and they ultimately decided to decline the transaction.

d. A bank that received an export LC from an overseas bank escalated the transaction because there was very little information about the applicant and beneficiary. The bank contacted the beneficiary who said that the goods were to be used in the manufacture of pharmaceuticals. So the bank requested the issuing bank to clarify certain details, including: the role of the beneficiary; whether the beneficiary was the supplier or an intermediary; the nature of the goods and the intended end-use; whether the end-use was consistent with the applicant's general activity; and whether any specific export licences were required. In response, the issuing bank asked the bank to discontinue handling the transaction. The bank declined the transaction and made a suspicious activity report to SOCA.

3.6.7 Using third-party services

123. Some of the banks in our sample used third-party services to help verify the details provided in trade documentation and determine whether a transaction might be suspicious. The use of third-party services varied across the sample. Some banks encouraged extensive use of third-party data sources and used them innovatively and creatively, while others did not use any.

> One bank gave the following guidance to trade processing staff: 'vessel checks should be conducted for any transaction which appears in your best judgement to be of a suspicious nature, regardless of amount'.

124. Most of the third-party services we observed banks using were free of charge. For example, a number of websites provide information about shipping vessels – including registration and ownership details, route information and recent ports of loading and discharge. Most of the major shipping lines also provide tracking facilities for containers and bills of lading on their websites; these are often free of charge and easy to use.

> One bank processed a transaction in which the documents presented showed that the goods were to be shipped from Jebel Ali in the UAE to Bangladesh. The team conducted a vessel check, which showed that the vessel had in fact departed from Bandar Abbas in Iran. The transaction was declined.

> A major bank validated container numbers on all bills of lading with an algorithm used by the industry to generate container codes[5], which had been built into its trade processing system.

125. Some banks considered the size of containers and whether the stated transport method in the documentation was consistent with the volume of goods being shipped. Where discrepancies were identified, further scrutiny was applied.

> A major bank initially had concerns about the container size for a shipment. It subsequently made enquiries with the shipper and the following comment was recorded on file: 'As for capacity, [the shipper] has upgraded their containers to carry a maximum payload of 28.8 metric tonnes, which is not exceeded in this case.'

126. A number of the banks used a service provided by the International Maritime Bureau (IMB) for checking whether shipments had taken place as described in the bill of lading. Details that could be verified included whether or not the cargo was loaded on to the ship in the quantity described, or whether the ship actually travelled on the route and date specified.

> One bank had carried out further enquiries on an export LC as the value of the transaction had exceeded a certain monetary threshold. The bank used the IMB's services to verify the information given in the bill of lading. They found that the quantity of goods shipped was different from that stated on the bill of lading. The exporter was also making repeated calls to the bank about the transaction, a tactic widely recognised as a possible red flag for banks to consider. On this basis the bank decided to exit the credit and raise a suspicious activity report.

5 There is an International Organisation for Standardisation (ISO) standard that applies to the identification of intermodal (shipping) containers (ISO 6346). This sets out how, using a particular algorithm, an identification code for a shipping container should be generated.

A bank advising an export LC issued by a Chinese bank raised concerns about a trade involving scrap copper, a high-risk product due to its volatile price. Suspicions were raised about the goods description (which gave the copper content as 99.5%) and because the value of the trade differed significantly from the beneficiary's previous transactions. Further investigation revealed that the beneficiary was acting as an agent and wanted to set up a 'back to back' LC in favour of an ultimate supplier. At this point, the transaction was referred to the IMB, who raised a number of concerns:

- they had not come across the beneficiary before in the context of copper trading
- the copper content value was too high for scrap
- the goods description was unusually vague
- an Institute of Scrap Recycling Industries specification had not been stated, and
- the market price of scrap copper at the time was around 9% higher than that stated on the LC, an indicator of possible under invoicing.

Ultimately the bank decided to reject this transaction.

127. The IMB issues bi-monthly bulletins to its members[6], which include details of recent frauds, commercial failures and non-payment of debts relevant to international trade. Banks may find this a useful source of information to help keep themselves up-to-date with the latest trade risks.

128. Some banks made significant efforts to look into the pricing of goods using a range of publicly available information sources. However, although prices are widely available for commodities such as oil, they are less readily available for others.

129. One bank told us about a transaction of rice that had been escalated because the value of the LC had breached a pre-determined monetary threshold. The bank identified that the market price was 20% higher than the price reflected in the LC. After investigating further, they declined the transaction on the suspicion that this might have been a case of under invoicing.

At a small foreign bank, we reviewed a number of back-to-back LC transactions involving a number of companies implicated in an investigation by an overseas central bank into irregularities in the purchase of 'all terrain' trucks for the country's military.

We found evidence to suggest that some of the firms involved might have been complicit in over invoicing using back-to-back LC payments that covered the same description and quantity of goods. We were concerned that the bank in question had not identified these issues with the pricing and structuring of the transactions. We have received confirmation from the bank's senior management that this business has now stopped.

3.6.8 Quality assurance

130. It is good practice for banks to conduct periodic reviews of transactions to assess whether trade processing staff are following the correct processes and making reasonable judgements about money laundering risks. Some banks had established specialist teams independent of the trade processing teams to perform this function. However, many banks had not carried out an internal audit review of their trade finance business.

One bank had a specialist team that was responsible for monthly audits of transactions processed by the trade team and for conducting a second review of transactions that had been escalated by trade processing staff. The monthly audits involved a complete re-performing of the process for a 10% sample of the previous month's transactions.

6 www.icc-ccs.org.uk/icc/imb/products/bulletin

131. Banks should ensure that those responsible for undertaking quality assurance are sufficiently qualified and experienced to do so. We found that some staff in compliance, internal audit and legal functions had a limited understanding of trade-based money laundering risks. This meant they were unable to oversee or challenge the business effectively on decisions taken. We also found that compliance and/or internal audit work usually focused on whether processes had been followed rather than whether reasonable judgements had been made by relevant staff.

> Quality assurance of trade finance business at one bank was conducted by a member of the offshore risk team. This individual could not articulate a basic understanding of key money laundering risks in trade finance. In addition, his testing did not include an assessment of whether trade processing staff considered money laundering risks when processing transactions.

132. Several banks relied on trade specialists to identify money laundering concerns. However, some banks' trade specialists did not have a good understanding of trade-based money laundering risk and were experts only in the Uniform Customs and Practice (UCP) rules and the technicalities of a transaction.

133. As a result, we were concerned that senior management in many banks might not have a true picture of money laundering risk in their trade finance business

3.6.9 What might a good transactional review look like for trade finance business?

134. We found that an effective approach to ensuring suspicious transactions are identified, escalated and scrutinised effectively would likely include the following stages. This is based on good practice we identified at a number of the better performing banks and is intended to help banks put adequate systems and controls in place, not to be prescriptive. Smaller banks will likely require fewer stages of review due to the smaller volumes of transactions involved.

a. A 'level 1' review by trade processors with a good knowledge of international trade, customers' expected activity and a sound understanding of trade-based money laundering risks, who are responsible for assessing money laundering risks in each transaction and escalate potentially suspicious transactions.

b. A 'Level 2' review by staff with specialist expertise to be able to further assess whether an escalation from a level 1 processor is a possible trade-based money laundering case. These teams are likely to require extensive knowledge of trade-based money laundering risk and make appropriate use of third-party data sources to verify key information.

c. A compliance/investigations team takes referrals from Level 2. These teams may conduct further investigations to determine if a transaction should be declined and if a SAR needs to be raised.

d. Regular quality assurance work is carried out to assess the judgements being made during this process. It would be good practice for this work to include transactions not escalated by level 1 processors as well as those that were.

3.6.10 Transaction anti-money laundering controls – good and poor practice

Good practice

- A formal consideration of money laundering risk is written into the operating procedures governing LCs and BCs.
- The money laundering risk in each transaction is considered and evidence of the assessment made is kept.
- Detailed guidance is available for relevant staff on what constitutes a potentially suspicious transaction, including indicative lists of red flags.
- 'Level 1' trade processors are employed with good knowledge of international trade, customers' expected activity and a sound understanding of trade-based money laundering risks.
- Processing teams are encouraged to escalate suspicions for investigation as soon as possible.
- Those responsible for reviewing escalated transactions have an extensive knowledge of trade-based money laundering risk.
- Underlying trade documentation is obtained and reviewed wherever possible.
- Analysis of pricing for those goods where reliable and up-to-date pricing information can be obtained.
- Regular, periodic quality assurance work is conducted by suitably qualified staff who assess the judgements made in relation to money laundering risk and potentially suspicious transactions.
- Where red flags are used by banks as part of operational procedures, they are regularly updated and easily accessible to staff.
- Expertise in trade-based money laundering is held in a department outside the trade finance business (eg, compliance) so that independent decisions can be made in relation to further investigation of escalations and possible SAR reporting.

Poor practice

- Failing to assess transactions for money laundering risk.
- Relying on customer due diligence procedures alone to mitigate the risk of money laundering in transactions.
- Relying on training alone to ensure that staff escalate suspicious transactions, when there are no other procedures or controls in place.
- Disregarding money laundering risk when transactions present little or no credit risk.
- Disregarding money laundering risk when transactions involve another group entity (especially if the group entity is in a high risk jurisdiction).
- Focusing on sanctions risk at the expense of money laundering risk.

- Failing to document adequately how money laundering risk has been considered or the steps taken to determine that a transaction is legitimate.
- Using trade-based money laundering checklists as 'tick lists' rather than as a starting point to think about the wider risks.
- Failing to investigate potentially suspicious transactions due to time constraints or commercial pressures.
- Failing to ensure that relevant staff understand money laundering risk and are aware of relevant industry guidance or red flags.
- Failing to distinguish money laundering risk from sanctions risk.
- Having ambiguous escalation procedures for potentially suspicious transactions, or procedures that only allow for escalation to be made to sanctions teams.
- Not taking account of other forms of potentially suspicious activity that may not be covered by the firm's guidance.
- Failing to make use of information held in CDD files and RMs' knowledge to identify potentially suspicious transactions.
- Not giving trade processing teams sufficient time to fully investigate potentially suspicious activity, particularly when there are commercial time pressures.
- Failing to make use of third party data sources where available and appropriate to verify information given in the LC or BC.
- Not encouraging trade processing staff to keep up-to-date with emerging trade based money laundering risks.

3.7 Sanctions and CTF controls

3.7.1 Introduction

135. In contrast to our findings on money laundering controls, most banks had more effective processes in place for managing the sanctions risks in their trade finance business.

136. Many banks told us greater focus had been placed on developing effective sanctions controls, as this was perceived as a higher risk for trade finance business.

137. Some banks did not distinguish between sanctions and money laundering risks and some banks referred to sanctions teams and sanctions training when we asked about money laundering.

One bank confirmed that they placed greater focus on sanctions risk than money laundering risk. This was because, in their opinion, even well-meaning customers might fall foul of sanctions rules. The same bank felt that, due to its stringent on-boarding processes, it was less likely that customers would engage in money laundering.

138. We were told that a focus on managing sanctions risk was probably due to the fact that potential sanctions breaches are easier to identify than potential cases of trade-based money laundering. Automated screening systems, when used properly, allow banks to compare high volumes of information contained in SWIFT[7] messages and other scanned documents to names on relevant sanctions lists quickly and efficiently. Conversely, none of the banks had automated systems that could identify potential trade-based money laundering.

139. In addition, the heightened level of regulatory scrutiny with regard to sanctions compliance (with large fines being issued where breaches have been identified) may also have led to some banks focusing attention on sanctions compliance at the expense of money laundering controls.

3.7.2 Screening process

140. Banks should screen transactions against applicable sanctions lists such as the Office of Foreign Assets Control (OFAC), the Treasury, United Nations (UN) and European Union (EU) lists. This list is not exhaustive and banks may choose to screen other relevant lists, depending on their customer base and geographical footprint.

141. Most banks followed a similar approach to sanctions screening. This included screening relevant SWIFT messages as well as underlying trade documentation. All but three banks had automated systems for screening SWIFT messages and, with the exception of one small bank, all conducted manual screening checks on the trade documentation. (Some banks had explored whether Optical Character Recognition software could be used to automatically extract names from trade documentation for screening. However, at the time of our review, none of the banks in our sample had managed to successfully integrate such a system into their screening process.)

142. Some banks developed their own internal 'hotlists' or 'watchlists', which they also screened. These usually comprised a list of counterparties a bank had chosen not to do business with. One bank updated its internal hotlist with information gathered from third-party sources, such as vessel checking websites.

143. With one exception, banks screened all fields in the payment and relevant BC and LC SWIFT messages. It was also common practice for amendments to LCs to be screened, with re-screening usually triggered by the receipt of new information or documentation.

144. Given the fluid nature of trade finance transactions, it is good practice for banks to have procedures that capture new or amended information received through the life of a transaction and to screen against all fields in trade and payment-related SWIFT messages.

145. Most banks supplemented automated sanctions screening with manual screening. This involved trade processing teams reviewing details of transactions (and the information contained within trade documents) and entering them into a sanctions screening system. Some banks would assess each transaction to see if they involved sanctioned entities and/or dual-use goods.

> One bank developed a spreadsheet for its trade processing team to analyse the details for each transaction and determine if an escalation was required on sanctions grounds. The spreadsheet guided trade processors to consider a number of sanctions-related factors, such as country risk, type of goods, screening of participants in the transaction and whether the goods were consistent with the customer's normal business. This process was in addition to automated SWIFT screening.

7 SWIFT – Society for Worldwide Interbank Financial Telecommunications

146. It is good practice for banks to ensure that information contained in underlying trade documentation (eg, commercial invoices, bills of lading), is screened against applicable sanctions lists and only one bank failed to screen this information. Some banks scanned trade documentation into their IT systems and then manually input that information into their sanctions screening software The main reason banks scanned documents was so that they could forward them to offshore document checking teams. Documents were not generally scanned for sanctions screening, although some banks were exploring this. At least two banks screened the documents received as part of a BC.

147. When a bank identifies a link to a sanctioned jurisdiction and/or entity (even if the parties identified are not the principal counterparties), this should be properly investigated and the decision whether or not to proceed with a transaction should be clearly documented. Banks may identify links to parties by reviewing documentation during a transaction.

> We reviewed a transaction at a major bank where the bank issuing an LC was part owned by an Iranian entity. There were also web searches on file identifying potential links with Syria. We were concerned that no additional checks had been conducted other than those on key parties (for which there were no hits).

3.7.3 Potential sanctions matches

148. Potential sanctions matches were generally reviewed by trade processing staff. They were usually able to review these 'hits' and close the ones they believed to be false positives.[8] It is good practice for staff to document their reason for closing down sanctions alerts. Among other things, this enables banks to assess whether staff are exercising correct judgements when discounting false positives by carrying out periodic checks.

> At one bank, each transaction was passed to a sanctions screening team in group compliance at certain key stages in the transaction's lifecycle or when new information was received by the bank (such as amendments to trade documents). This process was paper-based, with names of countries, addresses, ports, vessels and other details entered manually into the bank's sanctions screening software. Transactions could not proceed until this team had granted approval.

> One bank had a sanctions 'centre of excellence' team responsible for the first level review of transactions and administering the day-to-day operation of the automated screening software. Sanctions teams were aligned to product type; in relation to trade there was a specific point of contact assigned to provide advice on trade-related sanctions hits.

149. When trade processing staff did not consider hits to be false positives, they generally escalated them for a second review, usually conducted by a member of the compliance team or by a specialist sanctions unit. However, at some banks the second level review was conducted by a more senior member of trade processing staff before escalation to compliance or central sanctions teams.

8 Automated screening software works by attempting to match details input into the system against sanctions lists. Where the system identifies a potential match, it will raise a 'hit' that must be reviewed before the transaction can be processed. To take into account mis-spellings and translation issues, most screening software can be calibrated to allow hits to be generated even if the name put into the system is not an exact match with a name on a sanctioned list (this is often referred to as 'fuzzy matching'). This can cause hits to be generated by names of entities that are not sanctioned – a false positive.

One bank used a decision matrix to help staff determine whether or not to escalate a potential sanctions match. The matrix had four categories: individual, vessel, entity and location. If the name of a person triggered a hit on a vessel, for example, this could be cleared as a false positive. However, if the name of an entity matched a location then the matrix directed the processor to escalate. In all cases, a brief explanation of the decision taken was retained in the processing system.

The bank had also assessed that approximately 90% of true sanctions hits generated in their trade business over the last two years related to vessels. They therefore tailored the sanctions screening process so that potential matches with vessels were prioritised for review by trade processing staff. Other scenarios prioritised for review included exact name matches (as opposed to hits generated by fuzzy matching) for individuals, entities and vessels. This enabled the bank to be more focused in its review of potential matches.

3.7.4 Sanctions controls – good and poor practice

Good practice

- Screening information is contained within trade documents against applicable sanctions lists.
- Hits are investigated before proceeding with a transaction (for example, obtaining confirmation from third parties that an entity is not sanctioned), and clearly documenting the rationale for any decisions made.
- Shipping container numbers are validated.
- Potential sanctions matches are screened for at several key stages of a transaction.
- The review of certain types of potential matches is prioritised following analysis of previous sanctions alerts.
- Automated screening is supplemented by considering the sanctions issues as part of trade processing procedures.
- Ensuring new or amended information about a transaction is captured and screened.

Poor practice

- Staff dealing with trade-related sanctions queries are not appropriately qualified and experienced to perform the role effectively.
- Failing to screen trade documentation.
- Failing to screen against all relevant international sanctions lists.
- Failing 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.
- Failing to record the rationale for decisions to discount false positives.
- Failing to undertake screening for agents, insurance companies, shippers, freight forwarders, delivery agents, inspection agents, signatories, and parties mentioned in certificates of origin where this information is available, as well as the main counterparties to a transaction.

- Failing to record the rationale for decisions that are taken not to screen particular entities and retaining that information for audit purposes.

3.7.5 Counter terrorist financing (CTF) controls

Dual-use and high-risk goods

150. Dual-use goods include software, technology, documents, diagrams and other goods that can be used for civil and military purposes. They range from raw materials (eg, aluminium alloys) to components (eg, bearings) and complete systems, such as lasers. Specialist knowledge is often required to determine whether or not goods have a dual use. Dual-use goods are subject to export controls in the UK and are governed by the Department for Business, Innovation and Skills (BIS). A list of the goods subject to these controls is set out in the EU Dual-Use Regulation.[9]

A small bank listed certain types of high-risk goods within their policies that would warrant an escalation to compliance. However, during our visit we identified two transactions involving high-risk goods on this list that had not been escalated. One of these transactions involved an applicant involved in nuclear energy.

151. Most banks did not have systems and controls in place to identify and escalate transactions involving dual-use goods. We were often told that identifying dual-use goods was beyond the capability of most bank staff. However, while we recognise that this is a complex area, it is poor practice for banks not to consider measures to identify transactions involving dual use goods.

We were told by different banks that 'our staff are *not nuclear* scientists', 'our staff *don't have PhDs*', '*it's a challenge for banks to develop practical controls*' and '*there is a limit to what can be picked up*'.

152. Many banks told us that identifying dual-use goods depended on the knowledge and understanding that trade processing staff have about a customer. As a result, some banks set out the types of goods that staff should look out for and encouraged staff to escalate transactions where there was any doubt about whether they might involve dual-use goods.

One bank included within its customer due diligence procedures a section that set out more commonplace goods descriptions that might indicate terrorist financing, for example: 'centrifuges', 'pumps'; and 'homing devices'.

In contrast, a senior member of the trade processing team at another bank did not expect his team to understand a customer's business, adding that dual-use goods were not an issue as the bank's customers were well established.

153. At some banks, there were no high-risk/dual-use goods policies and procedures, while at others, the lists only focused on military goods or those that might have a 'lethal end use'. Some banks, with large volumes of trade finance business, tailored their approach to ensure that higher-risk transactions involving dual-use goods were identified and escalated.

9 Council Regulation (EC) No 428/2009 as amended by Regulation (EU) No 388/2012.

One bank told us that, because of the frequency of commercial transactions involving commonplace goods with a dual use, it was impractical to escalate transactions on the basis of the goods description alone. However, they did escalate transactions that had additional red flags such as:

- military or government buyers
- shipping to a known transhipment[10] destination or the shipping route is unusual for the product and destination
- the customer or purchasing agent is reluctant to offer information about the end use of the item
- the product's capabilities do not fit the buyer's line of business
- the packaging is inconsistent with the stated method of shipment or destination, and
- the item ordered is incompatible with the technical level of the country to which it is being shipped, such as semi-conductor manufacturing equipment being shipped to a country that has no electronics industry.

154. We found that the goods descriptions for some transactions could be limited and/or vague. To allow a proper assessment of the goods' potential use, it is good practice for banks to seek further information, either from counterparties to a transaction or from publicly available sources (see section 3.7.6 on third-party services).

At one bank the goods description for some transactions was very limited. The bank did not attempt to establish further details where terms such as 'scientific items' or 'spare parts' were used.

3.7.6 Third-party data sources

155. There are a number of publicly available sources of information that can be used by banks to help identify dual-use goods. These include:

a. The *Export Control – Checker Tools*[11] provided by BIS's Export Control Organisation. This is a useful tool for banks seeking to mitigate the risk of terrorist financing and allows banks to search against the relevant UK and EU dual-use goods lists. The Export Control Organisation can also be contacted directly for queries relating to dual use goods.

b. The European Commission's *TARIC database*, which allows users to identify if there are restrictions in place on a particular good. To identify restrictions using the TARIC database, users need the relevant product or 'TARIF' code for the item in question. This is often found on the commercial invoice.

3.7.7 Counter terrorist financing (CTF) controls – good and poor practice

Good practice

- Attempting to identify dual-use goods in transactions wherever possible.
- Ensuring staff are aware of dual-use goods issues, as well as common types of goods which have a dual use.
- Confirming with the exporter in higher-risk situations, whether a government licence is required for the transaction and seeking a copy of the licence where required.

10 Transhipment is the movement of cargo from one vessel (or other mode of transport) to another. Transhipment is often concentrated in transport hubs and free trade zones.

11 www.ecochecker.bis.gov.uk

Poor practice

- Failing to attempt to identify dual use goods in transactions.
- Focusing purely on military or 'lethal end use' goods.
- Not having a clear dual-use goods policy.
- Failing to undertake further research where goods descriptions are unclear or vague.
- Not making use of third-party data sources where possible to undertake checks on dual-use goods

4.

Consolidated examples of good and poor practice

This section consolidates examples of good and poor practice identified by this thematic review. These examples form the guidance material we are consulting on as part of this review. The next chapter states how this consultation will work. We welcome any comments you may have. The final text may differ from the material set out here; it may change to reflect comments and suggestions we receive.

Following consultation, we anticipate our final guidance on banks' handling of financial crime risks in trade finance activity will form a new Chapter 15 in Part 2 of *Financial crime: a guide for firms*. When published, it will be accompanied with brief introductory text setting out the context of this thematic review.

Financial crime: a guide for firms http://fshandbook.info/FS/html/FCA/FC/link sets out our expectations of firms' financial crime systems and controls and provides examples of the steps firms can take to reduce the risk of being used to further financial crime. We are committed to keeping the guide up-to-date. And we are required to consult on changes to 'guidance on rules' in the guide, such as relevant examples of good and poor practice from financial crime thematic reviews, which have not already been subject to consultation.

You may find it helpful to consider these examples of good and poor practice in conjunction with the 'About the Guide' section of *Financial crime: a guide for firms*. Among other things, this says 'Guidance should be applied in a risk based, proportionate way. This includes taking into account the size, nature and complexity of a firm when deciding whether a certain example of good and poor practice is appropriate to its business.'

Banks' control of financial crime risks in trade finance

Examples of good practice	Examples of poor practice
Governance and MI	
• Roles and responsibilities for managing financial crime risks in trade finance are clear and documented.	• There is a failure to produce management information on financial crime risk in trade finance. • There is a lack of internal audit focus on financial crime controls in trade finance. • The structure and culture of banks do not encourage the sharing of information relevant to managing financial crime risk in trade finance. • There is failure to establish appropriate forums to allow knowledge and information sharing about financial crime risk.
Risk assessment	
• Completing a documented financial crime risk assessment for trade finance business that gives appropriate weight to money laundering risk, as well as sanctions risk.	• Failing to update risk assessments and keep them under regular review to take account of emerging risks in trade finance. • Only focusing on credit and reputational risk in trade finance rather than carrying out a proper consideration of financial crime risk. • Not taking account of a customers' use of the bank's trade finance products and services in a financial crime risk assessment.
Policies and procedures	
• Staff are required to consider financial crime risks specific to trade finance transactions and identify the customers and transactions that present the highest risk at various stages of a transaction. • Staff are required to screen all relevant parties to a transaction.	• Very little money laundering guidance on financial crime risks specific to trade finance. • Staff are not required to consider trade specific money laundering risks (eg, FATF/ Wolfsberg red flags). • Procedures do not take account of money laundering risks and are focused on credit and operational risks. • No clear escalation procedures for high-risk transactions. • Procedures fail to take account of the parties involved in a transaction, the countries where they are based and the nature of goods involved.
Due diligence	
• Banks' procedures are clear about what checks are necessary and in what circumstances for non-client beneficiaries (or recipients) of an LC or BC.	• Written procedures do not make it clear what due diligence must be carried out on the instructing parties to an LC or BC depending on the bank's role in a transaction. • Trade processing teams do not make adequate use of the significant knowledge of customers' activity possessed by relationship managers or trade sales teams when considering the financial crime risk in particular transactions. • Lack of appropriate dialogue between CDD teams and trade processing teams whenever potential financial crime issues arise from the processing of a trade finance transaction.

Banks' control of financial crime risks in trade finance

Examples of good practice	Examples of poor practice
Training and awareness	
• Providing tailored training that raises staff awareness and understanding of trade-specific money laundering, sanctions and terrorist financing risks. • Using relevant industry publications to raise awareness of emerging risks.	• Only providing generic training that does not take account of trade-specific AML risks (eg FATF/Wolfsberg red flags). • Failing to roll out trade specific financial crime training to all relevant staff engaged in trade finance activity, wherever located. • Relying on 'experienced' trade processing staff who have received no specific training on financial crime risk.
AML procedures	
• A formal consideration of money laundering risk is written into the operating procedures governing LCs and BCs. • The money laundering risk in each transaction is considered and evidence of the assessment made is kept. • Detailed guidance is available for relevant staff on what constitutes a potentially suspicious transaction, including indicative lists of red flags. • 'Level 1' trade processor are employed with good knowledge of international trade; customers' expected activity; and a sound understanding of trade based money laundering risks. • Processing teams are encouraged to escalate suspicions for investigation as soon as possible. • Those responsible for reviewing escalated transactions have an extensive knowledge of trade-based money laundering risk. • Underlying trade documentation is obtained and reviewed wherever possible. • Third party data sources are used where appropriate to verify the information given in the LC or BC. • Analysis of pricing for those goods where reliable and up-to-date pricing information can be obtained. • Regular, periodic quality assurance work is conducted by suitably qualified staff who assess the judgements made in relation to money laundering risk and potentially suspicious transactions. • Trade processing staff keep up to date with emerging trade-based money laundering risks. • Where red flags are used by banks as part of operational procedures, they are regularly updated and easily accessible to staff. • Expertise in trade-based money laundering is also held in a department outside of the trade finance business (eg, Compliance) so that independent decisions can be made in relation to further investigation of escalations and possible SAR reporting.	• Failing to assess transactions for money laundering risk. • Relying on customer due diligence procedures alone to mitigate the risk of money laundering in transactions. • Relying on training alone to ensure that staff escalate suspicious transactions, when there are no other procedures or controls in place. • Disregarding money laundering risk when transactions present little or no credit risk. • Disregarding money laundering risk when transactions involve another group entity (especially if the group entity is in a high risk jurisdiction). • Focusing on sanctions risk at the expense of money laundering risk. • Failing to document adequately how money laundering risk has been considered or the steps taken to determine that a transaction is legitimate. • Using trade-based money laundering checklists as 'tick lists' rather than as a starting point to think about the wider risks. • Failing to investigate potentially suspicious transactions due to time constraints or commercial pressures. • Failing to ensure that relevant staff understand money laundering risk and are aware of relevant industry guidance or red flags. • Failing to distinguish money laundering risk from sanctions risk. • Having ambiguous escalation procedures for potentially suspicious transactions, or procedures that only allow for escalation to be made to sanctions teams. • Not taking account of other forms of potentially suspicious activity that may not be covered by the firm's guidance. • Failing to make use of information held in CDD files and RMs' knowledge to identify potentially suspicious transactions. • Not giving trade processing teams sufficient time to fully investigate potentially suspicious activity, particularly when there are commercial time pressures. • Failing to make use of third party data sources where available and appropriate to verify information given in the LC or BC. • Trade processing staff are not encouraged to keep up to date with emerging trade based money laundering risks.

Banks' control of financial crime risks in trade finance

Examples of good practice	Examples of poor practice
Sanctions procedures	
• Screening information contained within trade documents against applicable sanctions lists. • Hits are investigated before proceeding with a transaction (for example, obtaining confirmation from third parties that an entity is not sanctioned), and clearly documenting the rationale for any decisions made. • Shipping container numbers are validated. • Potential sanctions matches are screened for at several key stages of a transaction. • The review of certain types of potential matches is prioritised following analysis of previous sanctions alerts. • Automated screening is supplemented by considering the sanctions issues as part of trade processing procedures. • Ensuring new or amended information about a transaction is captured and screened.	• Staff dealing with trade-related sanctions queries are not appropriately qualified and experienced to perform the role effectively. • Failing to screen trade documentation. • Failing to screen against all relevant international sanctions lists. • Failing 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. • Failing to record the rationale for decisions to discount false positives. • Failing to undertake screening for agents, insurance companies, shippers, freight forwarders, delivery agents, inspection agents, signatories, and parties mentioned in certificates of origin where this information is available, as well as the main counterparties to a transaction. • Failing to record the rationale for decisions that are taken not to screen particular entities and retaining that information for audit purposes.
Dual-use goods	
• Attempting to identify dual use goods in transactions wherever possible. • Ensuring staff are aware of dual use goods issues, as well as common types of goods which have a dual use. • Confirming with the exporter in higher risk situations whether a government licence is required for the transaction and seeking a copy of the licence where required.	• Failing to attempt to identify dual use goods in transactions. • Focusing purely on military or 'lethal end use' goods. • Not having a clear dual use goods policy. • Failing to undertake further research where goods descriptions are unclear or vague. • Not making use of third party data sources where possible to undertake checks on dual use goods.

The previous chapter consolidates examples of good and poor practice identified by this review, which forms the guidance material on which we are consulting. Please see the Guidance Consultation {link in footnote} published simultaneously with this document for more details.

Please respond by: **4 October 2013**

You can send your response by email to: **carolin.gardner@fca.org.uk**

Alternatively, responses can be sent by post:
Carolin Gardner,
Financial Crime & Intelligence Department,
Financial Conduct Authority, 25 The North Colonnade, London, E14 5HS

Appendix 1
Examples of trade-based money laundering 'red flags'

The following are examples of trade-based money laundering red flags that were identified during our review. These may help banks think more clearly about potential financial crime risks in trade finance business. The list is not exhaustive and should not be relied on in isolation by banks when considering potential red flags.

Customer red flags

- The customer wishes to engage in transactions that lack business sense or apparent investment strategy, or are inconsistent with the customer's stated business strategy (eg, a steel company that starts dealing in paper products, or an information technology company that starts dealing in bulk pharmaceuticals).
- A customer significantly deviates from their historical pattern of trade activity (ie, in terms of value, frequency or merchandise).
- Transacting businesses share the same address, provide only a registered agent's address, or have other address inconsistencies.
- Pre-accepted discrepancy(s) by the applicant and/or the applicant is over-keen to waive discrepancy(s).
- Excessive/aggressive/pressured contact by the client.
- Customer is reluctant to provide clear answers to routine financial, commercial, technical or other questions.

Document red flags

- Shipment locations of the goods, shipping terms, or descriptions of the goods are inconsistent with the Letter of Credit. This may include changes in shipment locations to high risk countries or changes in the quality of the goods shipped.
- Significant discrepancies appear between the descriptions of the goods on the bill of lading (or invoice) and the actual goods shipped.
- Applicant-issued documents called for in the letter of credit.
- Unauthorised alterations/amendments to documents.

- Beneficiary or applicant refuses to provide documents to prove shipment of goods (possible phantom shipping or multiple invoicing).
- Bill of lading consigned: 'to be advised between applicant and beneficiary'. Consignment should be to a named party (usually the Applicant, Broker, Bank or to the order of shipper blank endorsed).
- Bill of lading describing containerised cargo, but without container numbers or with sequential numbers, non-standard numbers or indicates IRISL (Iran) prefix.
- LC includes a condition for a 'switch bill of lading'.
- Unusual codes, markings or stamps appear on monetary instruments, such as drafts or bills of exchange.
- Re-presentation of an official document immediately after a turn-down for discrepancy.
- Re-presentation of any shipping documents that were rejected because of US sanctions.
- Obvious alterations to third-party documents, eg, bills of lading, customs forms.
- Future dated bills of lading.
- LC received as unauthenticated SWIFT or untested telex message.

Transaction red flags

- Transaction structure appears unnecessarily complex and designed to obscure the true nature of the transaction.
- The transaction is an offshore shipment (eg, buyer/seller located in USA, while movement of goods occurred offshore of USA).
- Transaction involves an unusual intermediary or number of intermediaries.
- Significantly amended letters of credit without reasonable justification or changes to the beneficiary or location of payment. Any changes in the names of parties also should prompt additional OFAC review.
- The LC contains non-standard clauses, or phrases such as:
  - request to issue a 'ready, willing and able' message, or a 'letter of interest'
  - LC is 'unconditional, divisible and assignable'
  - transactions requiring 'proof of product'
  - funds are 'good, clean and cleared, of non-criminal origin'
  - bearer instrument letter of credit, or

  - transferable and assignable without being used.

- A party to a transaction is a shell company.
- Approach from previously unknown party whose identity is not clear, who appears evasive about their identity or connections or whose references are not convincing.

Payment red flags

- Unexplained changes to payment instructions.
- Request to pay a third party.
- The transaction involves the receipt of cash (or other payments) from third party entities that have no apparent connection with the transaction.
- Changing the LC or BC place of payment, eg, payment is to be made to beneficiary's account held in another country other than the beneficiary's stated location.
- Unusually favourable payment terms, such as payment substantially far above or below expected market price, interest rate substantially far above or below known prevailing rate, or lump-sum cash payment.
- The transaction involves an unusual trigger point for payment (eg, before goods are shipped, with no documentation required).
- Changing the LC beneficiary or BC payee name and address just before payment is to be made. Including requests for assignment of proceeds or transfer at the time documents are presented.
- LC or BC purportedly covers the movement of goods but fails to call for presentation of transport documents. LC covers steel shipment but allows a forwarder's cargo receipt (FCR).

Shipment red flags

- Trade transactions where the quantity of goods exceeds the known capacity of the shipping containers or the tanker capacity. Or where abnormal weights for goods are suspected.
- The shipment does not make economic sense. For example, the use of a forty-foot container to transport a small amount of relatively low-value goods.
- Shipping documents show weights and measures inconsistent with the goods shipped or method of shipment.

Glossary

Back-to-back LC – where the beneficiary of an LC arranges a second LC in favour of its own supplier, using the first LC as security.

Bill of lading – a document issued by a shipping company setting out the shipment details.

Letter of credit – a financial instrument issued by a bank that guarantees payment to a named beneficiary upon presentation of certain complying documents specified in the credit terms.

Bills for collection – process by which payment, or an accepted draft, is collected by a 'collecting' bank from an importer of goods for onward payment to the exporter. The collecting bank gives the relevant trade documentation (which will have been received from the seller, normally via the seller's [remitting] bank) to the importer in return. No payment obligations are assumed by the banks involved.

Dual-use goods – these include software, technology, documents, diagrams and other goods which can be used for civil and military purposes. They are subject to export controls in the UK.

Red flags – a detail/feature of a transaction that appears unusual and may, in isolation or in combination with other details, give rise to suspicions of financial crime.

Remitting bank – bank instructed by an exporter to send documents to the importer's bank as part of a documentary collection.

SWIFT – automated messaging system used by the financial services industry to send transaction details between parties. There are various SWIFT messages that specifically relate to Trade Finance, including the MT700 and MT400 series.

Trade-based money laundering – use of the international trade system to launder the proceeds of crime.

Financial Conduct Authority

PUB REF: 004720

25 The North Colonnade Canary Wharf
London E14 5HS
Telephone: +44 (0)20 7066 1000
Website: www.fca.org.uk