Chapter 15

Banks' control of financial crime risks in trade finance (2013)

15.1 Introduction

15.1.1 **Who should read this chapter?** This chapter is relevant, and its statements of good and poor practice apply, **to banks carrying out trade finance business**.

15.1.2 In July 2013, the *FCA* published the findings of our review of banks' control of financial crime risks in trade finance. We visited 17 commercial banks to assess the systems and controls they had in place to contain the risks of money laundering, terrorist financing and sanctions breaches in trade finance operations. Our review only considered Documentary Letters of Credit (LCs) and Documentary Bills for Collection (BCs).

15.1.3 We found that banks generally had effective controls to ensure they were not dealing with sanctioned individuals or entities. But most banks had inadequate systems and controls over dual-use goods and their anti-money laundering policies and procedures were often weak.

15.1.4 The following examples of good and poor practice should be read in conjunction with *FCG*. *FCG* provides more general guidance, including on AML and sanctions systems and controls, that can be relevant in the context of banks' trade finance business. Not all examples of good and poor practice will be relevant to all banks that carry out trade finance business and banks should consider them in a risk-based and proportionate way.

15.2 The FCA's findings

15.2.1 You can read the findings of the *FCA's* thematic review here: http://www.fca.org.uk/static/documents/thematic-reviews/tr-13-03.pdf

15.3 15.3Consolidated examples of good and poor practice

15.3.1 Governance and MI

Examples of good practice	Examples of poor practice
• Roles and responsibilities for managing financial crime risks in trade finance are clear and documented.	• Failure to produce management information on financial crime risk in trade finance.
• The bank ensures that staff have the opportunity to share knowledge and information about financial crime risk in trade finance, for example by holding regular teleconferences with key trade finance staff or by including trade finance financial crime risk as an agenda item in relevant forums.	• Internal audit fails to consider financial crime controls in trade finance.
	• The culture of a bank does not encourage the sharing of information relevant to managing financial crime risk in trade finance.

15.3.2 Risk assessment

Examples of good practice	Examples of poor practice
• The bank assesses and documents both money laundering and sanctions risk in the bank's trade finance business. This assessment is tailored to the bank's role in trade transactions and can form part of the bank's wider financial crime risk assessment.	• Failure 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.
	• Not taking account of a customer's use of the bank's trade finance products and

	services in a financial crime risk assessment.

15.3.3 Policies and procedures

Examples of good practice	Examples of poor 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 not required to consider trade specific money laundering risks (eg, FATF/Wolfsberg red flags).
• Staff identify key parties to a transaction and screen them against sanctions lists. Key parties include the instructing party, but may include other parties on a risk-sensitive basis.	• Procedures do not take account of money laundering risks and are focused on credit and operational risks.
• The bank provides guidance on recognising red flags in trade finance transactions.	• 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 the good involved.

15.3.4 Due diligence

Examples of good practice	Examples of poor practice
• Banks' written procedures are clear about what due diligence checks are necessary on the instructing parties. They take account of the bank's role in a transaction, and when it is appropriate to apply due diligence checks to others, including non-client beneficiaries (or recipients) of an LC or BC.	• 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.

15.3.5 Training and awareness

Examples of good practice	Examples of poor practice
• Tailored training is given that raises staff awareness and understanding of trade-specific money laundering, sanctions and terrorist financing risks.	• Only providing generic training that does not take account of trade-specific AML risks (eg FATF/ Wolfsberg red flags).
• Relevant industry publications are used to raise awareness of emerging risks.	• Failure to roll out trade specific financial crime training to all relevant staff engaged in trade finance activity, wherever located.
• Processing staff are trained to look for suspicious variances in the pricing of comparable or analogous transactions.	• Reliance on 'experienced' trade processing staff who have received no specific training on financial crime risk.

15.3.6 AML procedures

Examples of good practice	Examples of poor practice
• A formal consideration of money laundering risk is written into the operating procedures governing LCs and BCs.	• Failure to assess transactions for money laundering risk.
• The money laundering risk in each transaction is considered and evidence of the assessment made is kept.	• Reliance on customer due diligence procedures alone to mitigate the risk of money laundering in transactions.
• Detailed guidance is available for relevant staff on what constitutes a potentially suspicious transaction, including indicative lists of red flags.	• Reliance on training alone to ensure that staff escalate suspicious transactions, when there are no other procedures or controls in place.
• Staff processing transactions have a good knowledge of a customer's expected activity; and a sound understanding of trade based money laundering risks.	• Disregarding money laundering risk when transactions present little or no credit risk.
• Processing teams are encouraged to escalate suspicions for investigation as soon as possible.	• Money laundering risk is disregarded when transactions involve another group entity (especially if the group entity is in a high risk jurisdiction).
• Those responsible for reviewing escalated transactions have an extensive knowledge of trade-based money laundering risk.	• A focus on sanctions risk at the expense of money laundering risk.

• Underlying trade documentation relevant to the financial instrument is obtained and reviewed on a risk-sensitive basis.	• Failure to document adequately how money laundering risk has been considered or the steps taken to determine that a transaction is legitimate.
• Third party data sources are used on a risk-sensitive basis to verify the information given in the LC or BC.	• Trade-based money laundering checklists are used as 'tick lists' rather than as a starting point to think about the wider risks.
• Using professional judgement to consider whether the pricing of goods makes commercial sense, in particular in relation to traded commodities for which reliable and up-to-date pricing information can be obtained.	• Failure to investigate potentially suspicious transactions due to time constraints or commercial pressures.
• Regular, periodic quality assurance work is conducted by suitably qualified staff who assess the judgments made in relation to money laundering risk and potentially suspicious transactions.	• Failure to ensure that relevant staff understand money laundering risk and are aware of relevant industry guidance or red flags.
• Trade processing staff keep up to date with emerging trade-based money laundering risks.	• Failure to distinguish money laundering risk from sanctions risk.
• Where red flags are used by banks as part of operational procedures, they are regularly updated and easily accessible to staff.	• Ambiguous escalation procedures for potentially suspicious transactions, or procedures that only allow for escalation to be made to sanctions teams.
• Expertise in trade-based money laundering is also held in a department outside of the trade finance business (e.g. Compliance) so that independent decisions can be made in relation to further investigation of escalations and possible SAR reporting.	• Not taking account of other forms of potentially suspicious activity that may not be covered by the firm's guidance.
	• Failure to make use of information held in CDD files and RMs' knowledge to identify potentially suspicious transactions.
	• Trade processing teams are not given sufficient time to fully investigate potentially suspicious activity, particularly when

	there are commercial time pressures. • Trade processing staff are not encouraged to keep up to date with emerging trade based money laundering risks. • Failure to assess transactions for money laundering risk. • Reliance on customer due diligence procedures alone to mitigate the risk of money laundering in transactions.

15.3.7 Sanctions procedures

Examples of good practice	Examples of poor practice
• Screening information is contained within trade documents against applicable sanctions lists.	• Staff dealing with trade-related sanctions queries are not appropriately qualified and experienced to perform the role effectively.
• 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.	• Failure to screen trade documentation.
• Shipping container numbers are validated on a risk-sensitive basis.	• Failure to screen against all relevant international sanctions lists.
• Potential sanctions matches are screened for at several key stages of a transaction.	• Failure to keep-up-to-date with the latest information regarding name changes for sanctioned entities, especially as the information may not be reflected immediately on relevant sanctions lists.
• Previous sanction alerts are analysed to identify situations where true hits are most likely to occur and the bank focuses its sanctions resources accordingly.	• Failure to record the rationale for decisions to discount false positives.
• New or amended information about a transaction is captured and screened.	• Failure to undertake risk-sensitive screening of information held on agents, insurance companies, shippers, freight forwarders, delivery agents, inspection

	agents, signatories, and parties mentioned in certificates of origin, as well as the main counterparties to a transaction.
	• Failure to record the rationale for decisions that are taken not to screen particular entities and retaining that information for audit purposes.

15.3.8 Dual-use goods

Examples of good practice	Examples of poor practice
• Ensuring staff are aware of dual-use goods issues, common types of goods that have a dual use, and are capable of identifying red flags that suggest that dual-use goods risk being supplied for illicit purposes.	• No clear dual-use goods policy.
• 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.	• Failure to undertake further research where goods descriptions are unclear or vague.
	• Third party data sources are not used where possible to undertake checks on dual-use goods.