Financial Conduct Authority

Guidance consultation

Examples of good and poor practice in "Banks' control of financial crime risks in trade finance"

July 2013

1 Consultation

1.1 Our thematic review *Banks' control of financial crime risks in trade finance* explains the findings of our visits to 17 commercial banks to assess the systems and controls in place to contain the risks of money laundering, terrorist financing and sanctions breaches. This document is published simultaneously with this guidance consultation.

1.2 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.

1.3 We set out examples of good and poor practice in our thematic review. We propose to include these examples in a new chapter in Part 2 of *Financial crime: a guide for firms*, our regulatory guidance setting out our expectations of firms' financial crime systems and controls.

1.4 We believe that this guidance will make clear our expectations of firms' management of the financial crime risk associated with trade finance, improve the level of compliance across the sector, level the playing field for firms and ultimately lead to a reduction in financial crime.

1.5 By ensuring that UK banks put in place effective financial crime systems and controls, the incidence of money laundering, terrorist financing and sanctions breaches in UK trade finance should be reduced. This will also reduce the possibility that London's position as a

major financial centre is severely affected by money laundering, terrorist financing and sanctions breaches, for example through a major terrorist attack facilitated by funding channelled through the UK financial system.

1.6 Making it harder for illicit funds to pass through the UK financial system will increase the cost to criminals of moving illicit funds and the chance that they are caught. This will reduce the incentives for criminals to engage in such behaviour, and ultimately reduce the level of crime linked to moving illicit funds. Also, costs incurred by other agencies in preventing illegal behaviour may be able to be reduced.

1.7 The examples of good and poor practice we are consulting on are reprinted below for your convenience. We have not previously consulted on these examples. We welcome any comments you may have.

1.8 You can send your response by email to: carolin.gardner@fca.org.uk. Alternatively, responses can be sent by post to:

Carolin Gardner

Financial Crime and Intelligence

The Financial Conduct Authority

25 The North Colonnade

London E14 5HS

1.9 Please respond by 4 October 2013

2 Consolidated examples of good and poor practice

2.1 This section consolidates examples of good and poor practice identified by our thematic review *Banks' control of financial crime risks in trade finance.* These examples form the guidance material we are consulting on as part of this review. We welcome any comments you may have.

2.2 Following consultation, we anticipate that our final guidance will form a new chapter in Part 2 *of Financial crime: a guide for firms*. Once published it will be accompanied with brief introductory text setting out the context of the thematic review.

2.3 *Financial crime: a guide for firms* 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 have committed to keeping the guide up to date. We are also 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.

2.4 Readers 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 in the Guide 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 or 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.

Banks' control of financial crime risks in trade finance	
Examples of good practice	**Examples of poor practice**
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
Training and awareness	
• Providing tailored training 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)

Banks' control of financial crime risks in trade finance	
Examples of good practice	**Examples of poor practice**
• Using relevant industry publications to raise awareness of emerging risks.	• 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.	• 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

Banks' control of financial crime risks in trade finance	
Examples of good practice	**Examples of poor practice**
• 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.	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.ng trade based money laundering risks.
Sanctions procedures	
• 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	• 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

Banks' control of financial crime risks in trade finance	
Examples of good practice	**Examples of poor practice**
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.	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