Financial Conduct Authority

# Guidance consultation

# Proposed guidance on financial crime systems and controls

November 2014

# 1 Consultation

1.1 In November 2014 we published two thematic reviews. The first looked at 21 smaller banks' anti-money laundering (AML) and sanctions systems and controls.[1] The second was a review of the anti-bribery and corruption (ABC) systems and controls in ten wholesale insurance intermediaries.[2]

### Our AML and sanctions review

1.2 We assessed the adequacy of the AML and sanctions systems and controls of banks in our sample. We also considered to what extent the banks had considered our regulatory AML guidance, enforcement cases and the findings from our 2011 review of 'banks' management of high money laundering risk situations'. To this end, our sample included five banks that had also been part of our sample in 2011.

1.3 A small number of banks in our sample had implemented effective AML and sanctions controls. But despite our extensive work in this area over recent years, we found significant and widespread weaknesses in most of the sample banks' AML systems and controls and some banks' sanctions controls. We also found that AML resources were

[1] How small banks manage AML and sanctions risk – update
[2] Managing bribery and corruption risk in commercial insurance broking- update

inadequate in a third of all banks in our sample and that some overseas banks struggled to reconcile their group AML policies with UK AML standards and requirements.

## Our ABC review

1.4 As with our AML and sanctions review, we looked at sample intermediaries' ABC systems and controls and the extent to which those intermediaries had considered our existing ABC guidance, enforcement cases and the findings from thematic work, particularly our 2010 review of 'anti-bribery and corruption in wholesale insurance broking'. This sample also included five intermediaries that had been part of the sample in 2010.

1.5 While most intermediaries had begun to look at their ABC systems and controls, this was work in progress and more improvement was needed. We found that most intermediaries we saw were still not managing their bribery and corruption risk effectively. Business-wide bribery and corruption risk assessments were based on too narrow a range of risk factors and many intermediaries failed to take a holistic view of the bribery and corruption risk associated with individual relationships. Half of the due diligence files we reviewed were inadequate and senior management oversight was often weak.

## New guidance

1.6 Both reviews set out examples of good practice we observed. We propose to include these examples in two new chapters in Part 2 of our regulatory guidance, Financial crime: a guide for firms (the Guide).

1.7 We also propose to amend Part 1 of the Guide to clarify our expectations in some areas where significant weaknesses persist. In particular, we propose to include or amend existing text boxes in Chapters 2 and 3 on management information, risk assessments and enhanced due diligence and to change what we say in Annex 1 about source of wealth and source of funds.

1.8 Although the reviews focused on specific sectors, we believe that these amendments will help all authorised firms strengthen their financial crime systems and controls. It will also help firms approach financial crime compliance in a more proportionate and risk-based way that does not unduly restrict customers' or whole sectors' access to financial services: the risk-based approach does not require firms to deal generically with whole categories of customer or potential customer, and indeed greater risk-sensitivity will be achieved by assessing potential risk customer by customer.

1.9 On 28 October 2014 the FCA announced that its new Innovation Hub had started work, and identified a set of priorities for pro-innovation policy work. One of these to is to explore the difficulties met by innovative businesses when they seek to open bank accounts. In that connection we will wish to consider how far banks' approach to implementing the AML regime is a contributory factor, and whether there is scope to strike a better balance among the various considerations that influence the approach banks take.

1.10 We are required to consult on changes to guidance in the Guide because it constitutes 'guidance on rules'. This guidance is not binding and we will not presume that a firm's departure from our guidance constitutes a breach of our rules. We do, however, expect firms to take note of what our guidance says and, where appropriate, use it in a risk-sensitive way to inform their own financial crime systems and controls.

1.11 We welcome any comments you may have. You can send your response by email carolin.gardner@fca.org.uk

1.12 Please respond by 6 February 2015.

# 2 Financial crime guidance, including examples of good practice

2.1 This section lists the amendments we propose to make to the Guide. The guidance on which we are consulting is highlighted in **bold**. We will make consequential amendments to the Guide in our final guidance.

2.2 In this guidance, we use

- 'must' where provisions are mandatory because they are required by legislation or our rules;
- 'should' to describe how we would normally expect a firm to meet its financial crime obligations but we acknowledge that firms may be able to meet their obligations in other ways; and
- 'may' to describe examples of good practice that go beyond basic compliance.

### Amendments to Part 1 of the Guide

#### Part 1 Chapter 2: Financial crime systems and controls

2.3 We propose to introduce a new **Box 2.1A** on management information in our chapter on Financial crime systems and controls.

**Box 2.1A Management Information (MI)**

**MI should provide senior management with sufficient information to understand the financial crime risks to which their firm is exposed. This will help senior management effectively manage those risks and adhere to the firm's own risk appetite. MI should be provided regularly and ad hoc, as risk dictates**.

**Examples of financial crime MI include:**

- **An overview of the financial crime risks to which the firm is exposed, including information about emerging risks and any changes to the firm's risk assessment;**
- **Legal and regulatory developments and the impact these have on the firm's approach;**
- **An overview of the effectiveness of the firm's financial crime systems and controls;**
- **An overview of staff expenses, gifts and hospitality and charitable donations, including claims that were rejected;**
- **Relevant information about individual business relationships, for example:**
  - **the number and nature of new business relationships, in**

particular those that are high risk.
- **the number and nature of business relationships that were terminated due to financial crime concerns.**
- **the number of transaction monitoring alerts.**
- **details of any true sanction hits.**
- **details of any SARs considered or submitted.**

2.4 We also propose to amend **Box 2.3** on risk assessments.

**Box 2.3 Risk Assessments**

A thorough understanding of its financial crime risks is key if a firm is to apply proportionate **and effective** systems and controls.

**A firm should identify and assess the financial crime risks to which it is exposed as a result of things such as the products and services it offers, the jurisdictions it operates in, the types of customers it attracts, the complexity and volume of transactions and the distribution channels it uses to service its customers. Firms can then target their financial crime resources on the areas of greatest risk.**

**A business-wide risk assessment should:**
- **be comprehensive and consider a wide range of factors. It is not normally enough to consider just one factor;**
- **draw on a wide range of relevant information. It is not normally enough to consider just one source; and**
- **be proportionate to the nature, scale and complexity of the firm's activities.**

**Firms should build on their business-wide risk assessment to determine the level of risk associated with individual relationships. This should:**

- **enable the firm to take a holistic view of the risk associated with the relationship, considering all relevant risk factors; and**
- **enable the firm to apply the appropriate level of due diligence to manage the risks identified.**

**The assessment of risk associated with individual relationships can inform, but is not a substitute for, a business-wide risk assessment.**

**Firms should regularly review their risk assessments to ensure they remain current.**

Self-assessment questions:
- [...]

### Part 1 Chapter 3: Money Laundering and Terrorist Financing

2.5 We propose to amend **Box 3.7** in our chapter on money laundering and terrorist financing.

**Box 3.7: Handling higher-risk situations – enhanced due diligence**

Firms must apply EDD measures in situations that present a higher risk of money laundering. **MLReg 14**

EDD should give firms a greater understanding of the customer and their associated risk than standard due diligence. It should provide more certainty that the customer and/or beneficial owner is who they say they are and that the purposes of the business relationship are legitimate, as well as increasing opportunities to identify and deal with concerns that they are not. Box 3.3 considers risk assessments.

**The extent of EDD must be commensurate to the risk associated with the business relationship or occasional transaction but firms can decide, in most cases, which aspects of CDD they should enhance. This will depend on the reason why a relationship or occasional transaction was classified as high risk.** **MLReg 7**

**Examples of EDD include:**

- **obtaining more information about the customer's or beneficial owner's business**
- **obtaining more robust verification of the beneficial owner's identity based on information from a reliable and independent source**
- **gaining a better understanding of the customer's or beneficial owner's reputation and/or role in public life and assessing how this affects the level of risk associated with the business relationship**
- **carrying out searches on a corporate customer's directors or other individuals exercising control to understand whether their business or integrity affects the level of risk associated with the business relationship**
- **establishing how the customer or beneficial owner acquired their wealth to be satisfied that it is legitimate**
- **establishing the source of the customer's or beneficial owner's funds to be satisfied that they do not constitute the proceeds from crime.**

Self-assessment questions:
[...]

### Part 1 Annex 1: Common terms.

2.6 We will expand our description of 'source of funds and source of wealth in Annex 1 to Part 1. New text is in *italics.* As this text is not guidance on rules, it is not subject to consultation.

| | |
|---|---|
| Source of funds and source of wealth | As part of their customer due diligence and monitoring obligations, firms should establish that the source of wealth and source of funds involved in the business relationship or occasional transaction is legitimate. They are required to do so where the customer is a PEP.<br><br>'Source of Wealth' describes how a customer *or beneficial owner* acquired their total wealth. *This is distinct from identifying the assets they now own. Where necessary, the source of wealth can be verified on the basis of information and documents such as evidence of title, copies of trust deeds, audited accounts, salary details, tax returns or bank statements.*<br><br>'Source of Funds' refers to the origin of the funds involved in the business relationship or occasional transaction. *It refers to the activity that generated the funds, for example salary payments or sale proceeds, not the means through which the customer's or beneficial owner's funds were transferred.* |

## Amendments to Part 2 of the Guide

2.7 We propose to introduce two new chapters to Part 2 of our Guide. *Chapter 16: How small banks manage AML and sanctions risk – update*, will consolidate the examples of good practice identified in our thematic review 'how small banks manage AML and sanctions risk'. *Chapter 17: Managing bribery and corruption risk in commercial insurance broking- update* will consolidate the examples of good practice identified in our thematic review 'Managing bribery and corruption risk in commercial insurance broking- update'. The good practice in each chapter will be accompanied by a brief introductory text setting out the context of the thematic review as well as the major findings. We are consulting on these examples of good practice.

### Chapter 16: How small banks manage AML and sanctions risk – update

#### Management Information (MI)

**Useful MI provides senior management with the information they need to ensure that the firm effectively manages the money laundering and sanctions risks to which it is exposed. MI should be provided regularly, including as part of the MLRO report, and ad hoc as risk dictates.**

**Examples of useful MI include:**

- **An overview of the money laundering and sanctions risks to which the bank is exposed, including information about emerging risks and any changes to the bank's risk assessment.**
- **An overview of the systems and controls to mitigate those risks, including information about the effectiveness of these systems and controls and any changes to the bank's control environment.**
- **Legal and regulatory developments and the impact these have on the bank's approach.**
- **Relevant information about individual business relationships, for example:**
    - **the number and nature of new accounts opened, in particular where these are high risk**
    - **the number and nature of accounts closed, in particular where these have been closed for financial crime reasons**
    - **the number of dormant accounts and re-activated dormant accounts**
    - **the number of transaction monitoring alerts and suspicious activity reports, including where the processing of these has fallen outside of agreed service level agreements.**

### Governance structures

**Banks should put in place a governance structure that is appropriate to the size and nature of their business. To be effective, a governance structure should enable the firm to:**

- **clearly allocate responsibilities for financial crime issues**
- **establish clear reporting lines and escalation paths**
- **identify and manage conflicts of interest, in particular where staff hold several functions cumulatively**
- **record and retain key decisions relating to the management of money laundering and sanctions risks; including, where appropriate, decisions resulting from informal conversations.**

### Culture and tone from the top

**An effective AML and sanctions control framework depends on senior management setting and enforcing a clear risk appetite and embedding a culture of compliance where financial crime is not acceptable.**

**Examples of good practice include:**

- **Senior management taking leadership on AML and sanctions issues, for example through everyday decision-making and staff communications.**
- **Clearly articulating and enforcing the bank's risk appetite. This includes rejecting individual business relationships where the bank is not satisfied that it can manage the risk effectively.**
- **Allocating sufficient resource to the bank's compliance function.**
- **Ensuring that the bank's culture enables it to comply with the UK's legal and regulatory AML framework.**
- **Considering whether incentives reward unacceptable risk taking or compliance breaches, and if they do, removing them.**

### Risk assessment

**Banks must identify and assess the money laundering risk to which they are exposed. This will help them understand which parts of their business are most vulnerable to money laundering and which parts they should prioritise in their fight against financial crime. It will also help banks decide on the appropriate level of CDD and monitoring for individual business relationships.**

**MLReg 20 SYSC 6.3.1R**

**A business-wide risk assessment:**

- **Must be comprehensive. It should consider a wide range of factors, including the risk associated with the bank's customers, products, and services. It is not normally enough to consider just one factor.**

- **Should draw on a wide range of relevant information. It is not normally enough to consider just one source.**

- **Must be proportionate to the nature, scale and complexity of the bank's activities.**

**Banks should build on their business-wide risk assessment to determine the level of CDD they should apply to individual business relationships or occasional transactions. CDD will help banks refine their assessment of risk associated with individual business relationships or occasional transactions and will determine whether additional CDD measures should be applied and the extent of monitoring that is required to mitigate that risk. An individual assessment of risk associated with a business relationship or occasional transaction can inform, but is no substitute for, a business-wide risk assessment.**

**A customer risk assessment:**

- **Should enable banks to take a holistic view of the risk associated with a business relationship or occasional transaction by considering all relevant risk factors.**

- **Should be recorded. Where the risk is high, banks should include the reason why they are content to accept the risk associated with the business relationship or occasional transaction and details of any steps the bank is to take to mitigate the risks – such as restrictions on the account or enhanced monitoring.**

## Enhanced Due Diligence (EDD)

**The central objective of EDD is to enable a bank to better understand the risks associated with a higher risk customer and make an informed decision about whether to on-board or continue the business relationship or carry out the occasional transaction. It also helps the bank to manage the increased risk by deepening their understanding of the customer, the beneficial owner, and the nature and purpose of the relationship.**

**The extent of EDD must be commensurate to the risk associated with the business relationship or occasional transaction but banks can decide, in most cases, which aspects of CDD they should enhance.**

MLReg 7

**Senior management should be provided with all relevant information (e.g. source of wealth, source of funds, potential risks, adverse information and red flags) before approving PEP relationships to ensure they understand the nature of, and the risks posed by, the relationship they are approving.**

**Examples of effective enhanced due diligence measures we observed included:**

- **Obtaining more information about the customer's or beneficial owner's business.**

- **Obtaining more robust verification of the beneficial owner's identity on the basis of information obtained from a reliable and independent source.**

- **Carrying out searches on a corporate customer's directors (or individuals exercising control) to understand whether their business or integrity affects the level of risk associated with the business relationship, for example because they also hold a public function.**

- **Using open source websites to gain a better understanding of the customer or beneficial owner, their reputation and their role in public life. Where banks find information containing allegations of wrongdoing or court judgements, they should assess how this affects the level of risk associated with the business relationship.**

- **Establishing the source of wealth to be satisfied that this is legitimate. Banks can establish the source of wealth through a combination of customer provided information and documents such as: evidence of title, copies of trust deeds, audited accounts (detailing dividends), letters from employers confirming salary, tax returns, or bank statements. It is important for banks to establish how the customer or beneficial owner acquired their wealth, especially where they are a prominent PEP. This is distinct from identifying the assets they now own.**

- **Establishing the source of funds used in the business relationship to be satisfied they do not constitute the proceeds of crime. The source of funds refers to the activity that generated the funds; it does not refer to the means through which a customer's funds were transferred to the bank.**

- **Commissioning external third party intelligence reports where it is not possible for the bank to easily obtain information through open source searches or there are doubts about the reliability of open source information.**

- **Where the bank considers whether to rely on another firm for EDD purposes, it ensures that the extent of EDD measures is commensurate to the risk it has identified and that it holds enough information about the customer to carry out meaningful enhanced ongoing monitoring of the business relationship. The bank must also be satisfied that the quality of EDD is sufficient to satisfy the UK's legal and regulatory requirements.**

### Enhanced ongoing monitoring

**In addition to guidance contained in Part 1 Box 3.8 of *Financial crime: a guide for firms*:**

- **compliance have adequate oversight over the quality and effectiveness of periodic and event driven reviews**

- **The firm does not place reliance only on identifying large transactions and makes use of other 'red flags'**

***Transaction monitoring***

**Examples of red flags in transaction monitoring can include (this list is not exhaustive):**

- **third parties making repayments on behalf of the customer, particularly when this is unexpected**
- **repayments are made from multiple bank accounts held by the customer**
- **transactions are inconsistent with the business activities of the customer**
- **the purpose of the customer account changes without adequate explanation or oversight**
- **transactions unexpectedly involve high risk jurisdictions, sectors, or individuals**
- **early repayment of loans or increased frequency / size of repayments**
- **accounts with low balances but a high volume of large debits and credits**
- **cumulative turnover significantly exceeds the customer's income / expected activity**
- **debits are made shortly after credits for the same value are received**
- **the customer makes frequent transactions just below transaction monitoring alert thresholds**
- **debits to and credits from third parties where there is no obvious explanation for the transaction**
- **the customer provides insufficient or misleading information when asked about a transaction, or is otherwise evasive.**

***Customer reviews***

**Banks must keep the documents, data or information obtained as part of the CDD process up to date. This will help banks ascertain that the level of risk associated with the business relationship has not changed, or enable them to take appropriate steps where it has changed.**

**MLReg 8**

**Examples of factors banks may consider when conducting periodic reviews:**

- **Has the nature of the business relationship changed?**
- **Does the risk rating remain appropriate in light of any changes to the business relationship since the last review?**

- **Does the business relationship remain within the firm's risk appetite?**
- **Does the actual account activity match the expected activity indicated at the start of the relationship? If it does not, what does this mean?**

**Examples of measures banks may take when reviewing business relationships:**

- **assessing the transactions flowing through the customer's accounts at a business relationship level rather than at an individual transaction level to identify any trends**
- **repeating screening for sanctions, PEPs, and adverse media**
- **refreshing customer due diligence documentation, in particular where this is not in line with legal and regulatory standards**

### Sanctions

**In addition to guidance contained in Part 1 Chapter 7 of *Financial crime: a guide for firms,* examples of good practice include*:***

- **firms carry out 'four-eye' checks on sanctions alerts before closing an alert or conducting quality assurance on sanctions alert closure on a sample basis**
- **firms regularly screen their customer database (including associated persons) against sanctions lists using systems with fuzzy matching capabilities**
- **alert handlers have access to CDD information held on each of the bank's customers**

## Chapter 17: Managing bribery and corruption risk in commercial insurance broking – update

### Governance

- As part of their ABC governance structures, intermediaries may consider appointing an ABC officer with technical expertise and professional credibility within the intermediary.

### Management Information (MI)

Examples of ABC MI intermediaries may consider include:

- details of any business rejected in the relevant period
- details, using a risk-based approach, of staff expenses, gifts and hospitality and charitable donations, including claims that were rejected
- a breakdown of third party introducers and other intermediaries in the chain that are involved in business generation, with details of the business sectors and countries they work in
- the amount of business each third party introducer or other intermediary generates
- how much each third party introducer is paid and on what basis (fees, commission etc.)
- details of the third party introducer's role and why they are necessary

### Payment management information

Examples of payment MI that intermediaries may collect and consider include:

- How many third party introducers and producing brokers are involved in business generation?
- How much business does each one generate?
- How much is each one paid?
- What is each one's role?
- How many third party introducer and producing broker relationships are there?
- In which business sectors and countries do the third party introducers and producing brokers operate?
- Why is a third party introducer a necessary party in the chain?
- Reviewing payments to identify 'red flags' and unusual or suspicious payments.

### Risk assessment

#### *Business-wide risk assessments*

Intermediaries should identify and assess the bribery and corruption risk across all aspects of their business.

**Examples of factors intermediaries should consider when assessing risk across their business include:**

- **The risks associated with the jurisdictions the intermediary does business in, the sectors they do business with and how they generate business.**
- **The risks associated with insurance distribution chains, including the risk associated with parties that are not immediate relationships. These may include, in addition to the insured and the insurer, entities such as introducers, sub-brokers, co-brokers, producing brokers, consultants and agents.**
- **The risks arising from non-trading elements of the business, including staff recruitment and remuneration, corporate hospitality, and charitable donations.**

***Risk assessments and due diligence for individual relationships***

**The risk-rating process for individual third party introducer and client relationships, for example the producing broker, should build on the intermediary's business-wide risk assessment.**

**Examples of factors intermediaries may consider when assessing bribery and corruption risk associated with individual relationships include:**

- **the role that the party performs in the distribution chain**
- **the territory in which it is based or in which it does business**
- **how much and how the party is remunerated for this work**
- **the risk associated with the industry sector or class of business**
- **any political or governmental connections.**

**Intermediaries should decide on the level of due diligence, and which party to apply due diligence to, based on their assessment of risk associated with the relationship. This may include other parties in the insurance chain and not just to their immediate contact.**

**Examples of the type of information intermediaries may obtain as part of the due diligence process include:**

- **Other intermediary's terms of business and identification documentation.**
- **Checking, as risk dictates, on company directors, controllers and ultimate beneficial owners. Consider any individuals or company links to the client, PEP screening and status, links to a PEP or national government, sanctions screening, adverse media screening and action taken in relation to any screening hits.**
- **For third party introducers, details of the business rationale.**

### Ongoing monitoring and reviews

**Examples of ongoing monitoring and review for ABC purposes include:**

- **payment monitoring**
- **refreshing CDD documentation**
- **ensuring that the business rationale remains valid**
- **re-scoring risk**
- **updating PEP, sanctions screening, and adverse media screening**
- **taking a risk-based approach to ongoing monitoring measures applied to directors, controllers, ultimate beneficial owners and shareholders relevant to third party relationships, which is consistent with the risk rating applied at the outset of a relationship.**

### Payment controls – insurance broking accounts

**Intermediaries should set meaningful thresholds for gifts and hospitality that reflect business practice and help identify potentially corrupt actions.**

**When determining whether a payment is appropriate, staff responsible for approving payments should consider whether the payment is in line with expectations created by, among others, the due diligence held by the intermediary.**

### Payment controls – accounts payable

**Intermediaries should consider whether an absence of recorded gifts, entertainment, expenses and donations may be due to reporting thresholds being too high and/or staff being unaware of the requirement to report.**

### Training and awareness

**Examples of initiatives to supplement ABC training include:**

- **creating a one page "Aide Memoire" for staff. It listed key points about anti-financial crime and the whistleblowing process to which staff could easily refer**
- **appointing a compliance expert within each business area who provided ABC advice to staff**