The voice of banking
& financial services

21 September 2011

Tracey McDermott
Interim Director
Enforcement and Financial Crime Division
Financial Services Authority
25 The North Colonnade
Canary Wharf
London E14 5HS

Copy: cp11_12@fsa.gov.uk

Dear Sirs,

Re: Financial Crime: A guide for firms

The BBA is the leading association for the UK banking and financial services sector, speaking for 223 banking members from 60 countries on the full range of UK or international banking issues and engaging with 37 associated professional firms. Collectively providing the full range of services, our member banks make up the world's largest international banking centre, operating some 150 million accounts and contributing £50 billion annually to the UK economy.

We are pleased to have the opportunity to provide our comments on the FSA's proposals for a new regulatory guide on financial crime. We have discussed and agreed this response with all of our financial crime panels including MLROs of the largest banks, and medium and smaller banks also. We and our members would be happy to participate in any future discussions about our response and your proposed publication.

We have set out a selection of comments received on the specific questions raised in the consultation in the attached Annex A. We would like to preface these sets of comments with three additional views, first, on the timing of this publication, secondly on the content of the guide, and, thirdly on the status of the guidance.

1. Timing

The timing of this publication appears to us to conflict with all of the other significant policy and structural reform that is underway with financial crime in the UK. Not only are there various international initiatives (including the FATF review) but there is the HMT further consultation on the review of the Money Laundering Regulations 2007. We understand that there is also work being done on prosecution powers for economic crime (which is a hangover from the "legacy" of the ECA) and there are forthcoming Government strategies on fraud and cyber crime and the implementation of the NCA. We anticipate that with the focus of the Government on strategy, policy and powers,

British Bankers' Association
Pinners Hall
105-108 Old Broad Street
London
EC2N 1EX
T +44 (0)20 7216 8800
F +44 (0)20 7216 8811
E info@bba.org.uk
www.bba.org.uk

and the FSA focus on systems and controls, there may be many changes to the ways in which firms need to operate and prioritise financial crime controls. Many of the Government policies and plans are due imminently and we therefore believe that it would have been better to await the outcome and likely way forward than publishing this crime guide now.

2. Content

We note that the Guide is drawn from findings on FSA thematic reviews and splits into good practice and poor practice. However, the thematic reviews were carried out on very small parts of the financial industry and the application of findings from this narrow focus to the wider financial sector will be likely to inhibit a true risk based approach. The concept of good practice is beyond industry standard and in some cases might be described as best practice. It may drive firms to pursue good practice as defined by the FSA and not the appropriate level of control for their circumstances. This also appears to present a conflict with the drive by HM Treasury for industry to adopt a more risk based approach to anti-money laundering and to move away from a "tick-box" approach. We would therefore suggest that the statements of "good practice" are removed. Our members commented that statements of "poor practice" can be useful and enable them to confirm that their processes do not match any poor practice.

We have found throughout the Guide that some of the content is out of date and much of it lacks essential detail by way of legal basis or regulatory requirement that would make it useful. Furthermore, there are simply too many elements that need significant improvement for it to be useful in achieving its aims.

3. Status

On the question of the status of the guidance, we note the statement at paragraph 2.13 that "The guidance is not binding. Its status is that of any other FSA guidance. We will not presume that failure to follow a piece of guidance amounts, by itself, to a breach of our rules".

This statement runs contrary to Article 45(2) of the Money Laundering Regulations 2007 which states that; "In deciding whether a person has committed an offence under paragraph (1), the court must consider whether he followed any relevant guidance which was at the time – (a) issued by a supervisory authority or any other appropriate body;"

Given the status of the Guide it would seem that this would be defined as guidance under Article (45) and, as such, the contents of the Guide would be considered by the courts in determining if an offence has been committed. This presents the following potential issues:

- There is a risk that the contents of the Guide contradict or provide a different stance to that articulated by the JMLSG Guidance Notes. Examples of this are noted throughout our response, and;
- The comments in the "Good Practice" sections are, understandably, limited in their scope, however, the lack of detail could present challenges to financial institutions in arguing that their alternative controls are in compliance with the Regulations. Examples of this are noted throughout our response.

Whilst paragraph 2.15 of the CP indicates that; "The Guide is not intended to replace, compete or conflict with existing guidance on financial crime from other authorities or trade bodies.", the risks bulleted above will continue to exist unless the Guide states that where the Guide lacks clarity or there is a perceived conflict between it and another source e.g. the JMLSG Guidance Notes, the Guide will defer to that other source.

Overall therefore, we do not support the proposal to publish the Guide in its current form at the present time. For the reasons we have set out above, we do not find that Guide in its present form achieves its stated aims nor would it be useful to industry in achieving compliance with the totality of legal and regulatory requirements. The over-riding reason is, however, the lack of clarity around the status of the Guide and its conflict with the JMLSG guidance.

We hope that our comments are helpful and we would be happy to provide further details or clarification if needed.

Yours faithfully

Catriona Shaw
Director Financial Crime

Copy: Hugh Burns, HM Treasury
David Lewis, HM Treasury

Annex A

Questions listed in FSA CP11/12 "Financial Crime: a guide for firms"

Q1: Do you support our proposal to publish the Guide? If not, why not?

BBA Comment: we have covered this question in our opening comments on the timing of publication and on its status. Our members had various views, with some considering that it includes some useful and helpful material or believing it useful to the extent that it provides in a single document an amalgamation of a number of FSA thematic reviews and other documents. However, the findings of the thematic reviews were not subject to the challenge of a consultation process and cost benefit analysis. To produce guidance from these does circumvent some of the safeguards put in place to avoid gold plating the Regulations. Furthermore, some of the thematic reviews were carried out some time ago, eg on sanctions, and some of the practices noted by the FSA are no longer current practices in banks. Further, the Guide should set out, chronologically, the thematic work and studies undertaken by FSA prior to the FSA's creation of the Guide but which have contributed to it. This would help demonstrate to firms how these previous studies have helped for part of the control environment expected by FSA. However, overall, we do not support publication of the Guide at the present time.

Q2: Do you think the Guide will achieve our publication aims? If not, why not?

BBA Comment: we note that the three aims in publishing the guide were around transparency, accessibility and reinforcement. We believe that the real test of the effectiveness of the Guide which is not set out as an aim will be the extent to which it is used and found useful by firms. While the Guide does share some knowledge about FSA expectations, we found the structure confusing and as noted already the content is neither detailed nor is it sufficiently in tune with current market practices.

We believe that the transparency aim in particular falls far short of being met. The practice of identifying good and poor practice is well used by the FSA, but is unhelpful in many areas in not identifying the legal or regulatory source from which each practice point is derived. This is clearly set out in the JMLSG guidance and enables firms easily to trace guidance back to its source and it enables firms to consider the degree to which they need to apply it.

To achieve the aims set out, the Guide would have to be reviewed and updated frequently. For example, we note that some of the content is already 'stale', and it would have to keep up with changes to other industry best practice such as JMLSG, Wolfsberg, and the FATF.

On balance, publication of the guidance appears to be for the FSA's benefit, rather than for the regulated sector. We do consider that the preparation of this material which was originally to inform FSA supervisors has not translated well into guidance for the financial industry.

Q3: Do you consider that the Guide sets out with sufficient clarity which of its provisions apply to which firms? If not, how could we make it clearer?

BBA Comment: In the main, the Guide is clear in the overall introductory box before each chapter about which provisions affect which firms. However, some chapters could apply to more firms than listed. For example, chapter 9 on Countering weapons proliferation financing is particularly thin, and could have a wider scope in terms of the firms it covers, the types of activities and the countries to which they should apply caution.

There is uncertainty around the terminology used, for example what is the difference between "applies to" and "relevant to"? It would be clearer to use common phrases such as "This section applies to all firms".

Q4: Is the Guide's structure and the use of self-assessment questions, good and poor practice and cases studies, helpful and clear? How could we make it clearer or more useful?

BBA Comment: we found the structure of the Guide, in two parts to be unwieldy and confusing. In our view, the two parts should be combined. While we note the FSA's use of self assessment questions and "good and poor practices", the clarity of content is poor. For example, Box 8.1 states that "an individual of sufficient authority is responsible for adherence to the sanctions regime, but what constitutes "sufficient authority" is not expanded. We have already noted that it would be more useful to include the legal or regulatory source, and the guide would be more useful if the self assessment questions had answers on expected practice such as in box 2.5 throughout.

We also consider the Guide's structure could be improved if by including a specific section that outlines the different categories of firms that should review the Guide (wholesale, retail, international, insurance, brokers, asset management etc), with an accompanying definition for each category of firm. Specific guidance within the Guide can then better communicate what specific sections of the Guide apply what specific types of firm (please see our response to Question 3).

Q5: What other comments do you have about the structure of the Guide?

BBA Comment: Please refer to our answer to Question 3.

Q6: What comments do you have on the contents of the Guide? Do you have comments on the specific chapters or the annex of Part 1?

BBA Comment: we have a concern that by including subjects such as fraud, data security and bribery and corruption, that there may be an expectation on the part of the FSA that all of these subjects should be managed in the financial crime world. Some banks may manage these subjects and requirements in several different business areas, especially where they have to be applied across all parts of the business. We note that this is accepted at Box 2.2 but it remains a concern.

BBA Comment on Annex 1: A '419 fraud' is not co-terminous with 'advance fee fraud', it refers to the Nigerian penal code and is merely one particular version or style of advance fee fraud, there are others, notably prime bank instrument frauds and bogus commodity frauds.

We have the following additional points on Annex 1:

- Money Laundering Reporting Officer: it is an over-generalisation to say that the MLRO is 'also usually the "nominated officer"..' It would be preferable to say 'may also be the nominated officer…' In larger firms it would be quite unlikely that the same person fulfils both roles.
- 'posed by certain countries': incomplete ?
- placement etc: somewhat esoteric/untypical example of placement given.
- 3rd ML Directive: more accurate to say that the UK implemented *primarily* through the ML Regulations.
- There are various references to terms that are not otherwise used in any part of the Guide or consultation paper comments, so the purpose of their inclusion is unclear, for example:
  - Annex 1 financial institutions
  - FSRB/FATF style regional bodies
  - NCCT/Non-cooperative countries or territories;
  - Special Recommendations/FATF (Special Recommendations).

Comments on the contents of the Guide

1) Introduction

BBA Comment: please refer to our earlier comments on the status of the guidance. Specifically, we consider the Guide's overview could be improved by the inclusion of a specific section explicitly outlining the aims and objectives of the Guide.

2) Financial crime systems and controls

BBA Comment: there is little here that is surprising or imaginative although we were interested that this section contains so little on the compliance function and compliance surveillance. We would also like to emphasise that a risk-based approach to combating financial crime will mean a range of different approaches are taken - depending on the nature and characteristics of the firm in question.

On Box 2.1 Governance, there are some useful points, and the high level questions are worth including. There are some points that are not included such as whether ethical behaviour is embedded in the culture of the firm, and that regular discussions should be held with different business areas to discuss current risks/issues and to agree upon remediation and next steps.

Box 2.3 Risk Assessment is disappointingly thin. More information should be provided on what a 'good' risk assessment would involve because the scope and depth can be very wide ranging.

The guidance states that 'the firm actively considers the costs of crime to customers' but the impact of crime on customers is also important.

Box 2.4 Policies and procedures omits any suggestion that staff should be tested on their knowledge of policies and procedures.

3) Anti-money laundering (including guidance arising from the AML thematic review)

BBA Comment: we note that this chapter is set at a very high level. We would be surprised if even smaller banks and financial institutions found it to be helpful especially alongside the acknowledged industry standard which is, of course, the JMLSG guidance.

On Box 3.4 there is the erroneous implication that electronic checks for CDD are somehow inferior. It also is not operationally realistic to bulk check customers other than against a commercial PEP database in the absence of any official lists. On poor practice bullet 6, it is not clear in what respect this breaches the Regulations, which make specific reference to a 25% threshold when identifying beneficial owners. The FSA poor practice point implies firms are expected to go further than 25% in all cases. Further clarity is required.

We note also the statement that poor practice (bullet 5) that "the firm allows 'cultural difficulties' to get in the way of proper questioning to obtain necessary CDD information. Further clarification is needed on 'cultural difficulties'.

On Box 3.7 bullet 6, 'the firm disregards allegations of criminal activity from *reputable* sources', but there is no indication as to what might be considered a reputable source. Allegations from any source should be treated with caution until proven, particularly as some allegations, even those reported in the quality press might be libellous in nature.

The guide makes an incorrect statement that all high risk relationships are checked by the MLRO or their team. It is impractical for the MLRO or their team to review every single high risk case in large Groups.

On Box 3.8 it is not a question of lower alert thresholds per se (cf Box 12.4 thematic review says 'lower transaction monitoring alert thresholds'), but of calibrating monitoring tools to ensure greater scrutiny of higher risk customers. Bullet 1 states that 'key AML staff have a good understanding of information relating to a bank's highest risk/PEP customers.' This may not necessarily be appropriate for large banks and financial institutions that have a high number of PEP customers.

On Section 3.9 and reporting suspicions, it is agreed that a SAR should be clear and set out suspicions with appropriate detail to aid the authorities. However it is an unrealistic expectation of the FSA to assume that UK banks would be in possession of a customer's car registration details. This reference should be removed.

4) Countering terrorist financing

BBA Comment: our members found this section to be thin and very short of detailed practical guidance. The JMLSG guidance combines AML with CTF guidance throughout while also noting the key distinguishing features of both crimes eg paras 9-11 of JMLSG Preface. If the FSA wishes to include a section on CTF, we believe it must do much more on the following areas:

- the need for banks and other firms to conduct a detailed risk assessment and whether its business profile and customer base may make it vulnerable to use by terrorists;
- the need for banks etc to develop their own typologies in the light of any suspicions raised from their own business units or from any other readily available sources, and,
- whether existing CDD practices are sufficient to understand fully the types of its existing customer base that may give rise to the risk of terrorist financing.

On Box 4.1 bullet 4, there is material on "known terrorist groups…" but it is unclear as to what is meant by this statement. Banks have controls in place to check and identify designated/known terrorist groups, but what additional expectations does the FSA have on banks to identify terrorist groups?

On Box 4.1 bullet 5, there is a statement of poor practice that 'a firm assumes that terrorist funds flow only into the UK, and does not consider the risks of outbound payments being linked to terrorism. Further clarification is needed on what the FSA means by 'outbound payments'. Outbound payments would be made from the bank's own customers who would be checked against sanctions listings. What additional controls would the FSA expect a bank to implement on outbound payments?

Boxes 4.2 and 4.3 are very lacking in practical help. This section is essentially about FATF SRVII, and we have concerns about the presentation and interpretation by the FSA of expectations in this area. There is also no guidance on the internal use of abbreviations, acronyms, alternative spellings etc in watch lists to supplement official sanctions lists.

On Box 4.2, an intermediary bank is not required under Regulation 1781/2006 to chase up missing information nor would it be operationally realistic to expect it to do so, its obligation is only to pass on all the payer information it receives, whether complete or otherwise. (Highlighted box following para 327 of the thematic report seeks to imply an unrealistic obligation in this respect). See also comments below under Q7.

The 'peer discussions' (about persistently failing PSPs) is a somewhat aspirational recommendation in that currently no bespoke forum exists for the purpose. In view of the requirement to report such PSPs to the regulator, the FSA would logically be best placed to broker such discussions, indeed it is our recollection that there was previously some discussion of this possibility (which may be behind the comment in para 254 of the thematic report). See also JMLSG Part 3 Chapter 1 Annex 1/11, para 3.

Box 4.3 is especially weak and does not convey any particular message about good and poor practice in the area of CTF.

5) Fighting fraud (including guidance arising from the mortgage fraud thematic review)

BBA Comment: the majority of the focus here is on mortgage fraud. Banks have to tackle many other types of fraud, and we would suggest that the FSA needs to be careful not to give the impression that mortgage fraud is more important than other types of fraud, such as payment fraud, card fraud, cheque fraud. There is reference in the lenders section to "poor practice" including where a "lender fails to engage with the FSA's Information from Lenders" project. We are not aware of any consultation on this either with the CML or with the BBA.

There should be recognition given to the division between internal and external frauds. The guide does not set out to address fraud against the firm, but we believe it should do this.

Box 5.1: Preventing losses from fraud

The guidance should include that firms need to have a detailed fraud investigation procedure in place for handling fraud incidents from initial identification to completion. Information should be included on what a 'good' procedure would include, as well as a distinction between the immediate response and longer term remediation.

An additional self assessment question or good practice could be:

- the existence of a fraud monitoring programme which is reviewed on a regular basis;
- a reporting framework is in place for staff to report misconduct (noting alternative routes including Whistleblowing);
- Refresher fraud training should be reviewed on a regular basis (linked to guidance on training);
- Regular management information should be submitted to highlight current fraud risks/ issues. Fraud should also be a topic on the agenda to discuss with the business areas on a regular basis, and,
- Senior Management have responsibility for the anti-fraud measures in the firm.

An example of poor practice could be that a blame culture is created which discourages staff from reporting suspicious activity. As a structural point, this should include a reference therefore to guidance on reporting suspicions.

Paragraph 5.2 should include a reference to the Fraud Act 2006.

6) Data security

BBA Comment: The Guide claims to bring requirements forward from previous guidance, yet significant requirements laid out the FSA Countering Financial Crime Risks in Information Security from November 2004 are not included. If this document is designed to be a reference that is kept up to date, it would be better to bring forward all the data security requirements into a single reference, rather than leave a proportion of them to remain static and fall out of date. This is all the more pressing as the controls listed in the 2008 report are mainly based on internal threats, yet the threat of a persistent attack by external parties that would have serious consequences for a Financial Institution and its customers is rising. Examples of requirements listed in the 2004 paper but are not included in the Guide are:

- the control and management of firewall infrastructure;

- the control and management of wireless technologies;
- the control and management of intrusion detection systems;
- incident management;
- penetration testing;
- patch management.

Box 6.5 Poor practice bullet 4: the requirement that there should not be 'any password sharing of any kind' may provide technical difficulties with some systems used within Financial Institutions where passwords are shared 'under the covers' by systems and the process is transparent to users, e.g. in a scenario where two servers may process linked data. We suggest this might be better worded as 'individuals should not share passwords under any circumstances'.

7) Combating bribery and corruption

BBA Comment: the likelihood is that this chapter will be paid little attention by firms, given the more comprehensive nature of the Ministry of Justice's guidance, and the forthcoming BBA guidance. The BBA is working with our members to support implementation of the new Bribery Act. We aim to produce a document that sets out areas to consider for effective implementation this autumn. Topics that we are examining include due diligence, risk assessment, governance, policies and training and monitoring and review. As such, we may have more detailed comments to provide on the bribery section of the FSA guide as we progress our work in this area.

There is little mention of the Bribery Act 2010. Reference should be made to risks such as [foreign] public officials, third parties, agents, associated persons (not just customers but suppliers and agents etc), joint ventures, gifts and entertainment, and facilitation payments.

<u>By section:</u>

Box 7.2: Risk Assessment:

The box should include more about due diligence of customers, jurisdictions, PEPs, industry risk, product risk etc – the link to KYC should be emphasised.

The good practice would benefit from including more specific examples relating to the separate elements highlighted in the first self assessment question.

Remuneration structures should be considered in the guidance in terms of encouraging or discouraging business practices or strategies with respect to bribery risk.

The good practice points could include:

- Suppliers are classified by risk, i.e. high/medium/low and appropriate reviews are be conducted;
- Firms undertake an initial bribery risk assessment which is reviewed and updated on a regular basis;
- Adverse media checks on customers form part of the KYC process.

Box 7.3: Policies and Procedures:

Examples of good practice could include:

- 'policies are continually reviewed and have been updated in line with the Bribery Act 2010';

- ‘continual and comprehensive monitoring is carried out regarding internal and external risks facing the firm’, notably that this should not be about just monitoring the high risk issues and should be event driven.
- ‘actual or potential incidents of facilitation payments being requested or made are reported to an internal control function such as compliance’;
- ’Establishment of a policy pertaining to gifts, hospitality and entertaining which refers to bribery’ – not just monetary bribes.

Box 7.4: Dealing with third parties:

More mentions of Foreign Public Official risk, which are a risk presented along with third parties, would be helpful.

Additional guidance could be included on the process for approving third parties and the documentation of this process.

An example of good practice could be that the firm ‘maintains a central list of all third parties that it deals with and monitors this list for politically exposed person risk’.

Box 7.5: Staff recruitment, vetting and training:

In addition to assessing which staff are exposed to a higher risk of bribery, the firm should assess the methodology and assumptions behind this assessment, to ensure it remains relevant and effective.

The guidance could note in particular that training targeted at procurement staff is often forgotten.

It should also include that refresher training should be provided on a regular, event driven, basis and kept up to date. This is another important topic relying on good staff awareness as a significant line of defence.

An additional self assessment question or good practice point could be that a bribery assessment forms part of the new product approval process.

Box 7.6: Case study – corruption risk

The case study is good at drawing attention to the obvious bribery risks – third parties, high risk jurisdictions and a company with a deficit in controls – however the wording of the case study is too scant. Examples if they are able to be given of some weak controls may be useful. We suggest would be beneficial to have further cases studies, especially the most recent, Willis Limited.

8) Financial sanctions and asset freezes

BBA Comment: overall, we found this section to be particularly poor and in conflict in several areas with the JMLSG Guidance notes. In view of the fact that the FSA’s role in this area is confined to ensuring that firms have adequate systems and controls to meet the requirements of the asset freezing regime, we find that the Guide strays into other areas of general process and practice. For example, there is no legal or regulatory requirement that firms should carry out screening of persons or payments. Yet, in practice, this is how firms meet their requirements under the asset freezing regime. There is no guidance on the use of abbreviations, acronyms, alternative spellings etc in watch lists, to supplement official sanctions lists. SWIFT codes etc should also be used, not just the official list. The various boxes on screening are naively and dangerously incomplete in terms of what banks in practice have to do to meet their obligations. If the FSA believes it does have a role in

setting guidance on screening, we believe it needs to co-ordinate together with HM Treasury and with industry on what detail must be adhered to by relevant sectors of industry.

The FSA is nominated as the enforcement authority under Schedule 7 of the Counter Terrorism Act 2008; this responsibility, we assume, extends beyond solely ensuring firms have adequate systems and controls and thus should be reflected in the appropriate manner.

Box 8.1: Senior management responsibility: "Good practice : Senior management involvement in cases where a potential target match cannot easily be verified./Poor practice: No senior management involvement in cases where a potential target match cannot easily be verified.". The guidance that senior management (a term that can be widely interpreted) should be involved in the review of a potential target match, is at odds with the JMLSG Guidance on this issue. Part 3 Section 4.38 of the Guidance Notes states that; "potential matches should be reviewed by appropriately trained staff". From an operational perspective the JMLSG Guidance is the more practical guidance on this matter in particular for firms dealing with large numbers of potential target matches. Wording should be changed to follow that in the JMLSG Guidance Notes or be amended to be more in line with the wording in the fourth bullet in Box 8.7: Treatment of potential target matches.

Para. 8.2 provides an incomplete summary of financial sanctions obligations. A better summary is provided by 1.1.2 of the Thematic Review, although both fail to mention that it is an offence to 'deal' with assets belonging to, owned, held or controlled by designated persons.

Box 8.2: 'A UK firm operating in another currency has not considered whether it is subject to that country's financial sanctions regime' inaccurately suggests that the UK firm may be legally bound to comply with the other country's sanctions regime. Removal of 'whether it is subject to' corrects this misleading statement.

The footnote to 8.2 makes a reference to licences allowing insurance coverage. This example is too specific, and it implies the Licensing regime is only focused on allowing designated individuals to obtain insurance.

Box 8.3: Customer screening states that customers should be screened at take on. Good reasons are needed to justify retro screening. Clarification as to what is meant by their expectations – would screening within 24 hours of take-on be acceptable or would this be considered retro screening?

This also states that customers should be screened against HMT's Consolidated List. Does this imply that this is the only list or can banks and other financial institutions use an external supplier eg Worldcheck or Complinet, which incorporate the Consolidated List?

Box 8.3 also states that 'some firms may knowingly continue to retain customers who are listed under UK sanctions' is misleading because firms have no choice but to retain the relationship unless they obtain a licence from HM Treasury in order to 'deal' with the frozen funds, for example, to pay away to the customer. In addition, care should be taken not to contradict HM Treasury's preference that sanctioned persons should remain customers of a firm both when sanctions are in place and when they are lifted, albeit it a Financial Institution will generally seek to close these accounts on commercial / reputational grounds.

Good practice bullet point 3: 'able to identify similar spellings of names' does not encompass the full range of fuzzy matching considerations provided in the Thematic Review (para. 79) and the JMLSG guidance.

Good practice bullet point 6: this appears to relate to firms relying on another firm to carry out screening activity. There is, in fact, no reliance provision in the sanctions regulations and it would be wrong to suggest otherwise. The good practice comment in the FSA's Thematic Review, and replicated in similar wording here, has led to an increasing number of requests for detailed information about a firm's screening functionalities within the industry. Most of these firms do not

agree to be relied on in this regard and therefore are not usually willing, or even able due to confidentiality/ intellectual property considerations, to divulge the level of detailed information requested. If the statement refers to properly established outsourcing arrangements, this might be acceptable practice but this fact needs to be clarified.

Box 8.4: A 'false positive' also refers to names similar to watch persons, not just the same names (particularly taking into account naming practices within different cultures and different spellings used).

Good practice bullet 3: singling out 'claims handlers' seems to be an odd and narrow choice, particularly as this not included in the Thematic Review.

Poor practice bullet 2: this is incorrect and should be removed or amended to reflect the content of the Thematic Review. Not freezing an account is not a criminal offence - freezing an account is simply a control to prevent a criminal offence from occurring (e.g. to ensure funds owned, held or controlled by the designated person are not dealt with / not made available to the designated person).

Box 8.4: Good practice states that consideration should be given as to whether a breach should be notified to the FSA. Clarification is required as to when this should be done. If this was a Material Event, does this mean that there is a dual reporting obligation?

Box 8.5: Screening during client take-on: "Good practice: Screening against the Treasury list at the time of client take-on before providing any services or undertaking any transactions for a customer.". The guidance on this matter in the JMLSG Guidance Notes (Part 3 Sections 4.48-4.49) provides far greater clarity on this matter and more accurately articulates the conflicting challenges that firms face. The simplistic 'good practice' statement provides a different stance to that taken by the Guidance Notes, with the risk that the courts could find that a low risk business is in breach of the regulations because it failed to follow the FSA's 'good practice' statement.

"Good practice: The use of 'fuzzy matching' where automated screening systems are used.". There is no legal or regulatory obligation on a firm to apply 'fuzzy matching' and this term is not defined within the Guide. The JMLSG's guidance that firms "consider "fuzzy matching" and its explanation of what this can constitute, provides a clearer articulation of why 'fuzzy matching' could constitute 'good practice'.

Box 8.6: Ongoing screening: "Good practice : ensuring that customer data used for ongoing screening is up to date and correct.". Financial institutions are unable to "ensure" that this is the case. Client information changes on a regular basis and this may not be immediately apparent to the frequent institution (hence the introduction of a 'rolling review' of client information by many firms). It is suggested that the wording of this statement be amended.

"Good practice: Systems calibrated to include 'fuzzy matching', including name reversal, digit rotation and character manipulation.". See comments made in second part of section headed Box 8.5: Screening during client take on.

9) Countering weapons proliferation financing

BBA Comment: the limited information provided on this subject looks weak, and perhaps for presentational purposes would have been better included in the previous chapter on sanctions.

On application, this chapter is considered "most relevant to UK banks carrying out trade finance business", and also considers "project finance and insurance" as vulnerable. However, it should apply also to foreign banks operating in the UK, and to other types of banking business.

There are many obvious issues that are omitted and these include (but by no means represent all) the following:

- typologies
- the most obvious routes to look out for proliferation financing, such as free trade zones
- the need for banks to communicate with their clients about relevant regulations in place and how it may affect them
- EU Regulation 961/2010 prohibits indirect Iranian transactions. There is therefore a need for banks to look again at their clients and counterparties, especially clients that have a history of dealing with Iranian individuals and entities
- There is no mention of EU TARIC database.

We have three further points:
1. Box 9.1 'Does your firm finance trade with countries of concern, like Iran?': Beyond the obvious example of a country being subject to a relevant proliferation related UN or EU sanction (*i.e.* DPRK and Iran) it is unclear the basis upon which the FSA would determine whether a country is of concern. In the case of Iran and DPRK some element of mandatory legal obligation will be present, along with risks related to sanctions evasion by sanctioned entities, and proliferation financing by unsanctioned entities. Is it the FSA's intention that the net should be spread wider and include trade finance with potential transit countries (*i.e.* China, UAE, Malaysia, South Africa), or other countries where there is a concern over WMD proliferation (*i.e.* India and Pakistan). Given the complexity of this issue we would strongly urge the language is amended so as to stress that the most immediate indicator in determining the risk of whether a country is 'of concern' will be the presence of a relevant UN sanction *i.e. Iran and DPRK.*

2. Para 9.3: The final sentence in para 9.3 on reporting is somewhat confusing as it does not distinguish between the legal framework for making a CPF report using the SAR system in comparison to submitting a CPF related SAR for the purposes of Part 7 of POCA or under the Terrorism Act 2000 (TACT). The obligations and related legal safeguards vary significantly between the two reporting regimes and thus considerable care should be taken when dealing with this issue.

3. Para 9.4: In April 2010 the FATF published a February 2010 report from their Working Group on Terrorist Financing and Money Laundering '*Combating Proliferation Financing: A Status Report on Policy Development and Consultation'* which further analysed the risks associated with proliferation financing. We suggest adding a reference to this document.

A direct web link to SOCA's and HMT's guidance on proliferation financing reporting should be included.

The reference to the BIS Iran list does not solely include 'end users' who have had export licenses declined.

Q7: Is the inclusion of Part 2 of the Guide useful? What comments do you have on its contents?

BBA Comment: we believe that it would have been more useful to have a one-part Guide. If it is intended to go ahead with publication of this Guide, we would recommend updating the information in Part 2 and including this in the one document. The conciseness of the Part 1 chapters is at first glance a virtue, yet misleading since if as stated the examples in Part 2 have the same status as in Part 1 it is anomalous not to integrate them

Box 12.3: comment re 3.4 refers also. Using open source information may be a useful additional investigative tool but will not generally be a realistic means for the initial identification of a PEP in larger firms.

Box 12.4: global consistency in relation to exiting relationships needs to be qualified to allow for risk based exceptions.

Box 12.4: lower transaction alert thresholds, see above comment on Box 3.8.

Box 12.9: this section is flawed in conflating the obligations of intermediary and payee PSPs. The four bullet points are correct only in relation to Payee PSPs (and even then only partially, see below), **not intermediaries.** As to the 4th bullet and searching for meaningless information, firms' current system capablities for this purpose cannot yet be assumed.

Boxes 12.9 / 12.10 it follows that the titling and layout of these two sections needs to be corrected.

The expectation of the first bullet in 12.9 is unrealistic. Applying it to payee (beneficary) banks, other than for matches identified by sanctions screening, it can only be very exceptionally that payments are not processed, and then not usually purely for incomplete payer information. The industry made this point strongly via the BBA response to the consultation on the Common Understanding in relation to EC1781/2006 in 2008.

Box 12.11 bullet 4 systems limitations may preclude in short term searching in the way recommended, noting also that the introduction of the new cover message has no legal or regulatory underpinning beyond the Basel guidance document and that JMLSG does not include recommendations for monitoring of this sort and merely cross-refers for information to the Basel guidance.

Q8: Are there are topics not covered in the Guide which you would find it useful for us to address?

BBA Comment: It might be worth including e-crime

Q9: What comments do you have on our assessment of the equality and diversity issues we have identified?

BBA Comment: no comments, thank you.

Q10: Do you have any comments on this cost benefit analysis?

BBA Comment: no comments, thank you.