FSA

Financial Services Authority

Financial Services Authority

Anti-bribery and corruption in commercial insurance broking

Reducing the risk of illicit payments or inducements to third parties

May 2010

Contents

1. Executive Summary

1.1 Introduction

1. This report describes how commercial insurance broker firms ('broker firms') in the UK are addressing the risks of becoming involved in corrupt practices such as bribery. In particular, it sets out the findings of our recent review of standards in managing the risk of illicit payments or inducements to, or on behalf of, third parties in order to obtain or retain business. We published our interim findings in September 2009.[1] Although this work focuses on commercial insurance brokers, many of the issues covered and our examples of good and poor practice are relevant to firms in other sectors who use third parties to win business. We may do further work on anti-bribery and corruption in other sectors.

2. Firms' legal and regulatory responsibilities concerning anti-bribery and corruption are set out in Section 2.4. This report does not constitute nor should it be treated as our formal guidance. However, we expect firms to consider our findings, to translate them into more effective assessment of this risk, and to implement and maintain more effective appropriate controls where necessary. As in any other area of their business, firms should take an appropriate, risk-based approach to anti-bribery and corruption, taking into account relevant factors including their customer base, business and risk profile. Failure to do so may result in us taking action.

3. As a result of this review and our concurrent casework, we have commissioned a skilled persons report to assess past payments to third parties made by a firm and issued a formal private warning to another after we became aware of a number of third party payments which were made without an adequate business case being established and documented. We are considering whether further regulatory action is required in relation to other individuals and firms and it is likely that there will be referrals to Enforcement.

1.2 Findings

4. Although there were some examples of good practice, we identified a number of common concerns. These included:

   - Weak governance of anti-bribery and corruption efforts and a poor understanding of bribery and corruption risk among senior managers.

1 See: http://www.fsa.gov.uk/pages/About/What/financial_crime/library/interim.shtml

- Failure to implement a risk-based approach to anti-bribery and corruption in practice.
- Poor responses by many firms to significant bribery and corruption events which should have led them to reassess the adequacy of their preventative systems and controls.
- Very weak due diligence on, and monitoring of, third party relationships and payments with a worrying lack of documentary evidence of due diligence taking place. In particular, we found that:
  - many firms relied very heavily on an informal 'market view' of the integrity of third parties and took no steps to check the accuracy of account opening documentation;
  - few firms conducted detailed checking of higher-risk third parties to ensure they were not connected with either the assured, the client or public officials;
  - most firms had historically not taken any steps to establish and document the business case for using third parties in insurance transactions. However, there were signs this was changing;
  - most firms had historically not conducted regular reviews of their relationships with approved third parties;
  - several firms had not reviewed (or conducted their own) due diligence on third parties when teams or business were acquired from other firms;
  - there was no real consideration of whether payments made to third parties were commensurate with the services they provided;
  - some firms, acting on the instructions of third parties, had made payments to persons other than the approved third party without understanding or verifying the reasons behind the request;
  - in some firms, there was no independent checking of due diligence and the approval of third parties outside the producing department;
  - some firms did not have – and could not produce – a central list of third parties used to obtain or retain business. Others could not easily produce lists of payments made to third parties; and
  - most firms did not take adequate steps to confirm approved third parties' bank details, increasing the risk that they might unwittingly make payments to somebody else.
- Very little or no specific training was provided on anti-bribery and corruption, even for staff in higher risk positions.

- Although payment authorisation controls appeared generally adequate, virtually no firms took steps to identify unusual payments to third parties. As a result, some firms failed to report suspicious activity until after our visit or follow-up work.
- Inadequate compliance and internal audit monitoring of anti-bribery and corruption work.
- Weak vetting of staff compared with other financial sectors, with a heavier reliance on personal referrals and market gossip than usual.
- Although controls over staff expenses and accounts payable generally appeared to be effective, some firms gave large cash advances to staff to assist travelling in higher risk countries where they said credit cards were not readily accepted.
- Some firms awarded their brokers large bonuses directly related to the income or profit they generated. This could encourage risk-taking and negligence, and increase the risk of bribery and corruption, particularly where brokers use third parties to win business.

1.3 Conclusions

5. We have concluded that broker firms have approached higher risk business involving third parties far too informally and many firms are still not operating at acceptable standards. These firms need to do more to ensure they minimise the risk of becoming involved in bribery or corruption, unwittingly or otherwise. At present, we judge that the serious weaknesses identified in some broker firms' systems and controls mean there is a significant risk of illicit payments or inducements being made to, or on behalf of, third parties to win business.

6. We also believe that many firms are not currently in a position to demonstrate adequate procedures to prevent bribery – a defence to the Bribery Act 2010's new criminal offence of 'failing to prevent bribery'. However, we are encouraged by the progress of some broker firms over the past year in putting right weaknesses in their systems and controls, particularly through gap analysis against the interim findings of our review and the Final Notice we issued to Aon Ltd when we fined them in January 2009 for failing to establish and maintain effective anti-bribery systems and controls. We hope broker firms find the examples of good and poor practice in this document a useful tool for improving their systems and controls and raising awareness.

2. Introduction

2.1 Objectives

7. This report is the culmination of a significant project to examine how broker firms approach bribery and corruption risks, with a particular focus on reducing the risk of illicit payments or inducements to third parties in order to obtain or retain business. We investigated how broker firms assess and manage these risks, how risk management has changed during the past two years in light of significant external events and how the risks impact our statutory objectives.

8. The Financial Services and Markets Act (FSMA) defines financial crime 'to include any offence involving (a) fraud or dishonesty; (b) misconduct in, or misuse of information relating to, a financial market; or (c) handling the proceeds of crime'. The use of the term 'to include' means that this is not an exhaustive list and that FSMA can be interpreted widely to include bribery and corruption.

9. The risk of bribery and corruption is relevant to two of our statutory objectives:

   - *The reduction of regulated firms' vulnerability to financial crime* because weak controls over third party relationships and payments leave firms vulnerable to becoming involved in bribery and corruption, unwittingly or otherwise; and

   - *Market confidence* because bribery and corruption distort natural competition and could affect the UK's reputation, making it a less attractive place for firms to conduct insurance or other business.

10. Bribery and corruption was highlighted as an issue for firms in our *Financial Risk Outlook 2008*.[2]

> *'International efforts to combat corruption combined with the continuing development of the UK's legal framework on corruption may increase the level of interest in the financial services sector's efforts to combat corruption and bribery. There is a risk that firms could come under pressure to pay bribes, especially if they are operating in jurisdictions where paying bribes is widely expected. In addition, financial services firms may launder the proceeds of corruption or be used to transmit bribes.'*
>
> *FSA Financial Risk Outlook 2008*

2 http://www.fsa.gov.uk/pubs/plan/financial_risk_outlook_2008.pdf

2.2 Background

11. During our investigation of the Aon case in November 2007 (see box below), Thomas Huertas, who was then Acting Director of our Wholesale Business Unit, wrote to the CEOs of all broker firms. Our letter ('the Thomas Huertas letter') said: *"We are aware of some instances where wholesale insurance broker firms appear to have made illicit payments or inducements to, or on behalf of, third parties in order to obtain or retain business. This is unacceptable practice and so we are writing to all firms in this sector to set out our expectations in this matter and to ask firms to review their business practices to ensure that they are not involved in, or associated with, illicit payments."* We wrote this letter because the evidence gathered during the Aon investigation suggested that other firms may be involved in similar practices and have similar weaknesses in systems and controls.

In January 2009, we fined Aon Ltd £5.25 million for failing to take reasonable care to establish and maintain effective systems and controls to counter the risks of bribery and corruption associated with making payments to overseas firms and individuals.

Between 14 January 2005 and 30 September 2007, Aon Ltd failed to properly assess the risks involved in its dealings with overseas firms and individuals who helped it win business and failed to implement effective controls to mitigate those risks. As a result of Aon Ltd's weak control environment, the firm made various suspicious payments, amounting to approximately US$7 million, to a number of overseas firms and individuals.

12. In late 2008, our Wholesale Insurance Brokers Team requested that the Financial Crime Operations Team carry out a thematic review to assess how firms responded to the Thomas Huertas letter and how they try to mitigate the risk of bribery and corruption more generally.

13. The main purposes of the review were to gather information on current anti-bribery and corruption standards in broker firms; identify good practice to share with the industry; and highlight areas where firms need to improve. This report contains many examples of good and poor practice we observed during our fieldwork.

14. However, we expect firms to consider our findings, to translate them into more effective assessment of this risk, and to implement and maintain more effective appropriate controls where necessary. As in any other area of their business, firms should take an appropriate, risk-based approach to anti-bribery and corruption, taking into account relevant factors including their customer base, business and risk profile. Failure to do so may result in us taking action.

15. This is the first piece of thematic work we have conducted on anti-bribery and corruption. However, we may do further work on anti-bribery and corruption systems and controls in other sectors.

2.3 Methodology

16. The fieldwork for our review began in December 2008 and continued until January 2010. We visited 17 broker firms and consulted stakeholders including the City of London Police, the Serious Fraud Office, the Department for International Development and the Department for Business, Enterprise & Regulatory Reform. We also discussed anti-bribery and corruption standards in broker firms with forensic accountants and lawyers who had carried out extensive work on these issues.

> *"Corrupt payments [are] probably quite prevalent in broker firms"*
>
> *"Commercial insurance broking [is] a highly competitive market with narrow margins, especially in emerging markets. For these reasons, it would be difficult for a firm to compete with other firms making corrupt payments without also doing so."*
>
> *"This situation [is] exacerbated by the lack of enforcement of anti-bribery legislation in many higher risk countries."*
>
> *"These factors, in conjunction with a strong 'client is always right' culture, create…a 'toxic mix'"*
>
> Extracts from a discussion with a stakeholder

17. Our visits to firms began in January 2009 with our original intention to publish this report in July 2009. Our project was put on hold from April-November 2009 due to the secondment of key members of the project team to our Major Retail Groups Division to bolster the supervision of high impact firms. Because of this development, we rescheduled the remaining visits and published interim findings from the first ten visits in September 2009 which can be found on our website.[3] The remaining seven visits were conducted between mid-November 2009 and end-January 2010.

18. We obtained pre-visit information from all firms, including relevant policies and procedures; risk assessments; third party account opening forms; the firm's review of business practices following the Thomas Huertas letter; relevant Board and Committee minutes; and relevant internal and external audit reports. In addition, with the exception of the first four firms we visited, we obtained lists of payments made in the previous two years to overseas third party individuals or entities excluding loss payees, loss/claims adjusters and surveyors.

19. We interviewed staff with key roles in each firm to get a balanced view of how bribery and corruption risk was managed and identify at what level in the management structure it was dealt with. Where dedicated roles existed, we usually met staff ultimately responsible for anti-bribery and corruption; the officer nominated to make Suspicious Activity Reports (SARs); producing brokers dealing with higher risk business, particularly where it involved the use of third parties; and staff from accounts, human resources, compliance and internal audit.

3 http://www.fsa.gov.uk/pages/About/What/financial_crime/library/interim.shtml

20. We also discussed payments to third parties with producing brokers and other relevant staff, especially if the transaction appeared to be unusual and involved higher risk business. These included payments in a different currency from usual; those made to payees whose names were different from the account name; those made to individuals in high risk jurisdictions; and large, round sum payments when most others were not. We also examined files relating to third party accounts to ensure that the business case for making payments to third parties was fully understood within the firm and appropriately documented in line with the firm's policies and procedures.

21. We assessed the following matters in relation to anti-bribery and corruption:

- governance and management information (section 3.1);
- risk assessment and responses to significant bribery and corruption events (section 3.2);
- due diligence on third party relationships (section 3.3);
- payment controls for both insurance broking accounts and accounts payable (section 3.4);
- staff recruitment and vetting (section 3.5);
- training and awareness (section 3.6);
- risks arising from remuneration structures (section 3.7);
- incident reporting (section 3.8); and
- the role of compliance and internal audit (section 3.9).

22. We would like to thank the firms that participated in the review for the information they supplied before and during our visits. We would also like to thank the stakeholders for their advice and assistance.

2.4 Firms' legal and regulatory responsibilities

2.4.1 Legal obligations and the Bribery Act 2010

23. It is an offence under current UK anti-bribery legislation to give, agree to give or offer any gift or other consideration to a public official or an employee in the private sector as an inducement or reward for that person doing or not doing an act in relation to his principal's affairs or business. It does not matter whether the bribe is accepted or acted upon.

24. Since the introduction of the Anti-Terrorism, Crime & Security Act 2001 in February 2002, it has been illegal to bribe a person even if they have no connection with the UK.

This applies in all situations where the bribe constitutes an offence in the UK, even if the act is permitted in the country where it takes place. So, for example, where facilitation payments[4] are permitted in other countries, they would still constitute an offence under UK anti-bribery legislation. The penalties for bribery are up to seven years imprisonment and an unlimited fine for individuals and companies.

25. The Bribery Act 2010 received royal assent in April and will consolidate existing bribery legislation when it comes into force. It creates a new offence of 'failing to prevent bribery', which applies to commercial organisations or those performing services on their behalf. Under the Act, it will be a defence for a firm if it can demonstrate that it has adequate procedures to prevent bribery and the Government will publish non-statutory guidance on this. For FSA-regulated firms, our financial crime rules and principles will remain in force.

2.4.2 FSA rules and principles

26. Firms' regulatory responsibilities concerning anti-bribery and corruption are covered in our Principles for Businesses. Principle 2 requires that 'a firm must conduct its business with due skill, care and diligence' and Principle 3 that 'a firm must take reasonable care to organise and control its affairs responsibly and effectively, with adequate risk management systems'. Principle 1, which requires firms to conduct business with integrity, is especially relevant as broker firms and their employees may themselves be engaged in corrupt practices.

27. In line with these Principles, firms' senior management are responsible for making an appropriate assessment of financial crime risks, including those relating to bribery and corruption. The FSA rule SYSC 3.2.6R requires firms to '…establish and maintain effective systems and controls… for countering the risk that the firm might be used to further financial crime'. Firms therefore have a responsibility to assess the risks of becoming involved in, or facilitating, bribery and corruption and to take reasonable steps to prevent those risks crystallising.

28. Several firms and stakeholders have asked us to clarify when and how our rules and principles apply to business conducted overseas. Our regulatory powers apply in the following circumstances:

- if we can show that a firm's (or related third party's) actions overseas have negatively impacted UK market confidence;
- if a UK firm or one of its employees pays a bribe or makes a suspicious payment to an overseas person or in an overseas country; and
- if a UK firm fails to take reasonable steps to assure itself that third parties acting on its behalf are not making illicit payments to secure or retain business or otherwise acting in a corrupt fashion.

4 The Organisation for Economic Cooperation and Development (OECD) defines facilitation payments as those made to government employees to speed up an administrative process where the outcome is already pre-determined. They are illegal under UK anti-bribery legislation.

3. Findings

3.1 Governance and Management Information

29. Senior management awareness, involvement and responsibility are vital in ensuring adequate anti-bribery and corruption systems and controls are in place and that appropriate resources are allocated to mitigate identified risks.

30. We therefore assessed whether firms had a senior individual with overall responsibility for anti-bribery and corruption; the level of engagement in this topic on the part of the Board and any committees with responsibility in this area; and the extent to which the Board and committees received adequate management information.

31. We also assessed the quality of firms' policies and procedures relating to anti-bribery and corruption, how and when they were first established, and the involvement of senior management in ensuring they remain appropriate to mitigate the risks faced. In addition, we were interested in the results of firms' reviews of their business practices following the Thomas Huertas letter of November 2007 and, in particular, the way in which the reviews and any follow-up work were overseen by senior management. We also considered firms' responses and actions, particularly from a governance perspective, to the published findings relating to the Aon case in January 2009 and (where relevant) the publication of our interim findings in September 2009.

32. We found that a senior manager had formal responsibility for overseeing the risks of bribery and corruption at most firms we visited. However, we were concerned to find that, in more than half the firms visited, the relevant senior manager did not clearly understand the bribery and corruption risks faced by the business. As a result, most firms did not, in our opinion, carry out an adequate review of their systems and controls following the Thomas Huertas letter. For more on this, see Section 3.2.2.

33. In addition, when firms made improvements following the Thomas Huertas letter, the Aon case and the publication of our interim findings, changes to procedures were not always documented and/or communicated clearly to relevant staff. On occasions, this meant there remained a lack of clarity among front-line staff about the anti-bribery and corruption standards expected, particularly in their dealings with third parties.

At one firm, the Board received a monthly compliance report, but there was no evidence of any consideration of bribery and corruption risk. At another firm, we found very little evidence that financial crime issues were discussed by senior management.

3.1.1 The use of Management Information

34. Good, accurate Management Information (MI) is essential if a firm's Board and senior management are to assess, monitor and mitigate bribery and corruption risks. It is good practice for MI to cover new third party accounts, including risk classification, higher risk third party payments for the preceding period, changes to third party bank account details and general information about external developments relating to bribery and corruption.

35. Only four of the seventeen firms reviewed provided MI to senior management which allowed their Boards to form a clear view of how well they were managing bribery and corruption risk. We saw more evidence in these firms that bribery and corruption risks were discussed regularly at Board level.

One firm had no financial crime risks on their risk register and no financial crime issues had ever been discussed at Board level.

36. Four other firms produced a limited, but insufficient, amount of anti-bribery and corruption MI, sometimes as part of a wider compliance-type report. However, in the remaining nine firms, no relevant MI was produced at all. In these cases, anti-bribery and corruption was rarely discussed during Board meetings. This was very surprising given the increased focus on anti-bribery and corruption in recent years.

In a case we dealt with outside our project, one firm used two third party individuals to introduce high risk business. Despite these third parties presenting themselves to prospective clients as belonging to the firm, the firm received no MI to demonstrate that illicit payments were not being made to win business.

37. In several cases, we found management were unclear about the types of MI that would help them oversee anti-bribery and corruption work. This was often compounded by old or inflexible IT systems that could not easily produce useful information. This was often because higher risk third parties, such as introducers, were grouped with lower risk third parties such as clients, reinsurers, solicitors and loss adjusters.

Two firms had to produce a schedule of third party payments made over the previous two years as a special exercise for our visit, as this did not form part of their regular MI. In one case, the schedule provided contained inaccuracies.

3.1.2 Governance and Management Information - examples of good and poor practice

Good practice

- Clear, documented responsibility for anti-bribery and corruption apportioned to either a single senior manager or a committee with appropriate terms of reference and senior management membership, reporting ultimately to the Board.

- Good Board level and senior management understanding of the bribery and corruption risks faced by the firm, the materiality to their business and how to apply a risk-based approach to anti-bribery and corruption work.
- Swift and effective senior management-led response to significant bribery and corruption events, which highlight potential areas for improvement in systems and controls.
- Regular MI to the Board and other relevant senior management forums.
- MI includes information about third parties, including (but not limited to) new third party accounts, their risk classification, higher risk third party payments for the preceding period, changes to third party bank account details and unusually high commission paid to third parties.
- MI submitted to the Board ensures they are adequately informed of any external developments relevant to bribery and corruption.
- Actions taken or proposed in response to issues highlighted by MI are minuted and acted on appropriately.

Poor practice

- Failing to allocate official responsibility for anti-bribery and corruption to a single senior manager or an appropriately formed committee.
- A lack of awareness and/or engagement in anti-bribery and corruption at senior management or Board level.
- Little or no MI sent to the Board about higher risk third party relationships or payments.
- Failing to include details of wider issues, such as new legislation or regulatory developments, in MI.
- IT systems unable to produce the necessary MI.

3.2 Risk Assessment and responses to significant bribery and corruption events

3.2.1 Risk assessment and the implementation of risk-based systems and controls

38. Broker firms often deal with a very wide range of countries, classes of business and third parties. They should therefore consider adopting a risk-based approach to achieve optimum risk mitigation with their finite resources.

39. It is good practice for broker firms to focus on countries regarded as higher risk in terms of bribery and corruption, using tools such as the Transparency International Corruption Perceptions Index (the CPI).[5] They should also consider which sectors are higher risk, because of factors such as large contracts, high levels of competition, the use of third parties to win business and state involvement. Examples of classes of business generally regarded as higher risk are aviation and energy; however firms should consider whether other classes of business have characteristics which might heighten the risk of bribery and corruption. Factors that may increase the risk posed by third parties are covered in Section 3.3.1.

One firm which specialised in marine insurance had previously used the JCC Cargo Watchlist as a reference point for assessing the risk of bribery and corruption. The JCC Cargo Watchlist is a tool for identifying high risk countries in terms of war, terrorism and hijack when transporting cargo. It does not take into account bribery and corruption risk so this was not an appropriate tool for the firm to use.

40. Failure by firms to adopt a risk-based approach may result in inadequate risk mitigation for high risk business. It may also mean that time and resources allocated to risk mitigation will not be deployed in the most efficient way.

41. We found most firms had carried out some form of risk assessment relating to illicit payments, usually in connection with their response to the Thomas Huertas letter or subsequent external events. However, we found that few firms then applied a risk-based approach by focusing on higher risk jurisdictions, classes of business or third parties. Most firms adopted a 'one size fits all' approach to their systems and controls, which was frequently insufficient in addressing financial crime risk posed by third party relationships.

42. In many cases, broker firms started by plotting the countries where they used third parties to win business against the CPI in order to assess country risk. Many firms then categorised their third parties as high, medium or low risk; this was entirely dependent on the positioning on the index of the third party's country.

Some firms had very unsophisticated methods of using the CPI to assess country risk. One simply regarded the top 60 countries as low risk, countries 61-120 as medium risk and those placed lower than 121 as high risk. The firm did not consider the scores attached to each country. Had they done so, they would have noticed that, on a scale of 0 (corrupt) to 10 (clean), all the countries placed below position 50 on the CPI score less than 5.

43. In many cases, other factors, such as the class of business the third party operated in, whether the third party was an individual or a corporate entity, and the results of due diligence were not factored into the bribery and corruption risk assessment.

5 See: http://www.transparency.org/policy_research/surveys_indices/cpi/2009

44. Only two firms demonstrated risk assessment processes which took account of factors other than country risk and then took a more robust approach to dealing with higher risk business. In general, firms were unsure how to score risk, and many compliance departments appeared ill-equipped to advise effectively on risk rating.

One firm had implemented procedures where third party account applications from higher risk countries needed approval by the CEO or Chief Risk Officer, whereas other senior managers could approve other accounts. This firm also had more robust procedures in place for the approval of third parties who were individuals.

45. Many firms did not have documented procedures setting out additional procedural steps to be taken for higher risk third party accounts. In most cases, firms simply assessed their risk level based on the country's CPI score, and then carried out the same monitoring and due diligence for all accounts. Some firms told us that a higher risk CPI score would lead to more robust due diligence on new third party accounts; however they could not demostrate this happened in practice.

3.2.2 Firms' responses to significant bribery and corruption events

The Thomas Huertas letter

46. In November 2007, during our investigation of the AON case, Thomas Huertas wrote to the CEOs of all broker firms. Our letter asked firms to review their business practices to ensure that they were not involved in, or associated with, illicit payments. The ways in which firms responded to that warning and the extent to which they successfully planned, implemented, and completed the reviews, is therefore central to this project.

47. Broker firms' responses to the Thomas Huertas letter have shed considerable light on their ability to identify and assess bribery and corruption risks, the quality of governance, and their ability to manage internal projects aimed at overhauling systems and controls.

48. It is therefore extremely disappointing that, of the seventeen firms visited, only six carried out what we consider to have been an adequate review of systems and controls in response to the Thomas Huertas letter. Of the remainder, two firms made some improvements but without conducting a full review, and the remaining nine firms carried out little or no work in response to the Thomas Huertas letter. This was often because they considered their anti-bribery systems and controls to be broadly adequate; in most cases, this assessment was incorrect.

One firm conceded to us that their response to the Thomas Huertas letter had been inadequate. An action plan had been agreed in December 2007, but had not been completed when we visited in early 2009. Due to this lack of progress, the firm appointed an independent contractor shortly before our visit to review third party procedures.

49. In many cases, firms failed to carry out effective reviews of their business practices due to a lack of knowledge and awareness of bribery and corruption risk and how to mitigate it. This was evidenced when, during our visits, some firms expressed difficulty in understanding how bribery and corruption risks were relevant to their business when there were, in fact, significant risks.

50. Where internal reviews led to no improvements or only very small-scale changes, we found no evidence of challenge at Board level to ensure those carrying out the reviews were raising standards to a sufficiently high standard. This suggested that those at Board level did not have a clear understanding of bribery and corruption risk assessment and mitigation, or were not adequately interested.

51. Two firms appointed external consultants to conduct reviews in response to the Thomas Huertas letter. In both cases, a full set of recommendations were agreed and implemented in full. However, one firm initially relied on internal audit to conduct the review work, before realising it had insufficient in-house expertise to conduct an adequate review.

One of the firms in our project carried out a review, led by the Compliance Officer, in response to the Thomas Huertas letter, but made no changes to systems and controls. Following the publication of our interim findings and the appointment of a Compliance Consultant, the firm made some improvements. This suggests the firm itself was not adequately aware of the bribery and corruption risks or how they can be mitigated.

The Aon case and our interim findings

52. In January 2009, the FSA fined Aon Ltd £5.25 million for failing to take reasonable care to establish and maintain effective systems and controls to counter the risks of bribery and corruption.

53. Most firms carried out work on anti-bribery and corruption following the Aon case and several performed a gap analysis comparing their systems and controls with the weaknesses highlighted in our Enforcement Notice. Overall, we found firms responded quicker and more effectively to the Aon case than the Thomas Huertas letter.

Following the Aon case, one firm was asked by its overseas parent to produce, as a very high priority, a paper assessing the adequacy of systems and controls around third party relationships.

54. We carried out the last seven visits of our review after our interim findings were published in September 2009. In all but one case, we found that firms made further improvements following our interim findings. Although it was difficult for us to identify improvements directly attributable to our interim findings (as opposed to the Aon case and the Thomas Huertas letter), it was clear that our interim findings gave firms further impetus to improve their anti-bribery and corruption systems and

controls. While we were encouraged by the positive effects of the Aon case and our interim findings, it was worrying that few firms responded adequately to the Thomas Huertas letter.

55. Overall, we found firms' improvements to anti-bribery and corruption controls were too slow over the past few years, especially considering the increased focus on the subject. In several cases, firms were still implementing improvements to their systems and controls at the time of our visits. And, in a number of other cases, improvements had only been implemented a few days before we arrived, even though the firms had had up to two years to do so. In these cases, we could only assess how effective these new arrangements were theoretically, rather than practically.

56. Interestingly, many firms with stronger controls (and those that were making significant improvements) had often used a combination of consultancy support and guidance arising both from the Aon case and our interim review findings. This highlighted a significant training and awareness requirement. Training and awareness is covered in greater depth in Section 3.6.

Future events

57. It is good practice for firms to assess continuously whether external events may help them to refine their risk assessments and anti-bribery and corruption systems and controls. Examples of events which may give firms opportunities to reassess their control environments include the publication of this report; the publication of details about relevant regulatory or law enforcement action; and the publication of guidance from the Government relating to the Bribery Act 2010.

3.2.3 Risk assessment and responses to significant bribery and corruption events – examples of good and poor practice

Good practice

- Regular assessments of bribery and corruption risks with a specific senior person responsible for ensuring this is done, taking into account the country and class of business involved as well as other relevant factors.
- More robust monitoring and due diligence on higher risk third party relationships.
- Thorough reviews and gap analyses of systems and controls against relevant external events, with strong senior management involvement or sponsorship.
- Ensuring review teams have sufficient knowledge of relevant issues and supplementing this with external expertise where necessary.
- Establishing clear plans to implement improvements arising from reviews, including updating policies, procedures and staff training.

- Adequate and prompt reporting to the Serious Organised Crime Agency (SOCA) and us of inappropriate payments identified during reviews.

Poor practice

- Failing to consider the bribery and corruption risks posed by third parties used to win business.
- Failing to allocate formal responsibility for anti-bribery and corruption risk assessments.
- A 'one size fits all' approach to third party due diligence.
- Failing to respond to external events that may draw attention to weaknesses in systems and controls.
- Taking too long to implement changes to systems and controls following analysis of external events.
- Failure to bolster insufficient in-house knowledge or resource with external expertise.
- Failure to report inappropriate payments to SOCA and a lack of openness when dealing with us concerning any material issues identified.

3.3 Due diligence on third party relationships

3.3.1 What is a 'third party' and why do they pose a risk of bribery and corruption?

58. It is good practice for firms to define in their policies and procedures exactly what constitutes a 'third party'. Firms should also ensure all relevant employees understand the definition and the due diligence required in relation to establishing and maintaining relationships with third parties, particularly if they are higher risk.

At one firm, we found worrying confusion among key members of staff about how due diligence on third party relationships should be conducted. Although the Finance Director and Chief Operating Officer believed a certain form needed to be filled in by third parties, neither the individual responsible for recommending the opening of third party accounts nor a producing broker knew the form existed. It therefore appeared no standard third party form was being used and there was very little or no due diligence on the third party relationships we examined.

59. As a starting point, it is good practice for firms to regard all companies and/or individuals involved in insurance transactions who are not the underwriter or the assured to be third parties.

60. However, it is also important that firms focus their resources efficiently and effectively to minimise the risk of bribery and corruption. Therefore, firms should consider which types of third parties pose the greatest risk of bribery and corruption, and take this into account when refining the definition.

Identifying higher risk third parties

61. Third parties who provide services to refer, assist or facilitate the introduction of the client or the assured are likely to pose a higher risk of bribery and corruption. There is likely to be an increased risk of a third party being the recipient of a bribe or paying a bribe to others from commission received if:

- *It is an individual (or a 'company' which is in fact an individual)* – this is because an individual is more likely to be the ultimate recipient of a bribe and, generally, it is likely to be more difficult for an individual to influence a client to place insurance business with a particular broker firm.
- *It is introducing business from a country which is higher risk from a bribery and corruption perspective* – paying bribes can be regarded as 'how business is done' in some higher risk countries and there could be inadequate anti-bribery and corruption legislation and/or enforcement of it.
- *It is connected to the assured, the client or a public official* – this increases the risk that corrupt means could be used to win business, particularly if those to whom the third party is connected have influence over procurement decisions.
- *There is not a convincing business case for the third party to receive commission or the amount of commission paid appears high compared with the amount of work they do* – it is important for firms to understand fully the role of a third party and the services they provide so they can satisfy themselves that they are not making or becoming involved in illicit payments where the case for paying a third party is unclear.
- *It is paid commission on the instructions of another party involved in the transaction* – in these circumstances, broker firms could be being used by another individual or entity to pay bribes to the third party.
- *The third party does not want others involved in the transaction to know it will receive commission* – this lack of transparency increases the likelihood of bribery and corruption.
- *The third party requires payment of commission in advance of premiums being paid* – here, there is a risk that the commission could either be a bribe or passed on to others as a bribe to secure the business.

62. This list of higher risk factors is not exhaustive and firms should consider other characteristics which may increase the risk of bribery and corruption.

Care required when dealing with third parties which are usually lower risk

63. Examples of third parties likely to pose a lower risk of bribery and corruption are brokers, clients, reinsurers, solicitors and loss adjusters who are regulated within the EEA or by us. However, we are aware of situations where these types of third parties carry out higher risk activities such as introductions or referrals. It is therefore essential that firms clearly understand the role of third parties such as clients, reinsurers, solicitors and loss adjusters in all transactions, and define and treat them as a higher risk third party where appropriate.

3.3.2 Understanding and documenting the business case for payments to third parties

64. As discussed in paragraph 61, it is good practice for firms to ensure there is a convincing business case for a third party to receive commission. This reduces the risk of a firm making or becoming involved in illicit payments. However, we found due diligence on third party relationships to be generally very weak. In some cases, there was a worrying lack of documentary evidence of due diligence, which suggested that it had not been carried out at all.

As part of routine supervision, we asked a large broker firm to review past payments to third parties following the Aon case. The broker firm's review identified forty-eight transactions where the independent reviewer was unable to conclude a valid business reason for the transaction. All but one of these transactions was in a single broking department.

The firm's follow-up work to establish a business reason for these transactions identified eighteen where the only way it could ascertain a business case was to rely on an oral explanation from the account handling broker, as there was no supporting documentation. In some cases, the account handling broker who provided the explanation of business case was not the account handler at the time of the transaction.

65. Many firms relied very heavily on an informal 'market view' of the integrity of third parties and very basic checks to confirm the identity of third parties, such as printing third parties' websites (which are, of course, easy to forge). In addition, although many firms required third parties or their brokers to complete account opening forms, most firms did not check the accuracy of the third party's information, even where there was an increased risk of bribery and corruption.

One firm relied very heavily on a letter allegedly from the assured as due diligence on a third party relationship. However, the letter was not dated, the firm did not know when or how it was received, there was no name to confirm the author and the signature was not legible.

66. Another common issue was that third party account opening forms did not contain relevant questions. We observed several instances where third parties - who were individuals - were asked to fill in forms clearly aimed at corporate entities and contained very few questions relevant to an individual.

One firm provided us with their third party account opening form. It was entirely focused on corporate entities and was insufficient for use with third party individuals. The information it requested was: name; address; annual report and accounts; certificate of incorporation; origin of business; years trading; names of directors; and bank account details. It failed to request for any type of third party: a description of the services provided; the level of commission to be paid; or the business case for using them. The firm said they intended to make the form more suitable for individuals following our visit.

67. Often, we found that forms did not clearly state which sections were mandatory. Consequently, forms were often not fully completed. In addition, we observed that forms were sometimes completed with very vague information, particularly about the business case. In some worrying cases, incomplete forms or forms lacking sufficient detail to justify third party relationships were approved by senior management or compliance as the basis for opening third party accounts.

During one visit, we saw what appeared to be several attempts to improve the quality of third party files very shortly before our visit. One third party file contained very little due diligence – just a few contact details, a bank account number and an extract of the third party's website printed the day before our visit. For two other third parties introducing business from higher risk countries, the relevant Managing Director showed us files containing very little evidence of due diligence and admitted that 'paperwork was lacking'. These files contained commission sharing agreements sent to the third party on the day of our visit. Copies of files we took from the firm showed third party accounts were sometimes opened on the basis of an email stating that '(The third party) will introduce business to us'.

68. It is good practice for those responsible for approving third party accounts to ensure forms are completed correctly and in sufficient detail. Failure to do so indicates breaches of FSA Principle 2 (due care, skill and diligence) and Principle 3 (management and control). In order to ensure forms are appropriately completed and a convincing business case is documented, firms should consider using somebody with no prior knowledge of the proposed insurance transaction to review third party forms and other due diligence. It was our impression that in some firms, incomplete or vague explanations of the business case for using third parties were signed off because the approver had a good knowledge of the proposed transaction, felt it was legitimate, and overlooked deficiencies in documented due diligence.

69. We also saw some examples where firms, acting on the instructions of approved third parties, had made commission payments to others without understanding or verifying

the reasons behind the request. The result of these weaknesses was that, in many cases, due diligence on third party relationships or requests to make third party payments was simply not sufficient to establish the level of bribery and corruption risk.

A broker firm was instructed by a higher risk third party (Company A) to pay commission to Company B, which was based in another country. The broker firm did not independently verify the reasons behind Company A's instruction to pay commission to Company B, despite the reason being relatively simple – Company A said Company B was its sister company. The broker firm made four payments totalling $60,000 to Company B in less than a year even though it had not been approved as a third party. Only one commission payment for $28,000 was made directly to Company A.

70. Although most firms had not historically taken adequate steps to establish and document their business cases for using third parties, there were signs this was changing. Several firms either had or were introducing new third party account opening forms or strengthening existing ones, particularly following the Aon case. We strongly encourage firms that still do not establish and document convincing business cases for using third parties to strengthen their procedures.

Following receipt of the Thomas Huertas letter and a subsequent internal audit review of relevant business practices, as well as assessment of the Aon Final Notice, one firm introduced new questions on its third party account opening form relating to the business case, the services provided by the third party and the basis of the third party's remuneration.

3.3.3 Identifying third party connections to the assured, clients or public officials

71. Potential conflicts of interest inherent in payments to third parties connected with the assured, clients or public officials increase the risk that such payments could be illicit. We were therefore disappointed to find that few firms conducted checks to determine whether third parties might have such connections.

72. Several firms asked third parties to declare these kinds of connections on their account opening forms. However, many of these firms' third party account opening forms had been recently introduced or overhauled following high-profile events like the Aon case and, historically, most firms were not asking these kinds of questions. In any case, most firms which now asked for such connections to be disclosed took no steps, even in higher risk situations, to check the accuracy of information provided by the third party, particularly where no connections were disclosed.

One firm which derived the majority of its brokerage from a high risk class of business in a high risk country made a significant payment to a charity in that country on a shareholder's instruction. Despite the payment being unusual in the context of its normal third party payments, the firm did not fully investigate the identity of all the charity's trustees.

The firm showed us a parliamentary notice in a foreign language giving details of the trustees. However, there was no proper translation of the document and the directors who authorised the payment did not have more than a basic understanding of the foreign language. When questioned, the directors admitted they did not know who some of the trustees were.

Following the visit, we established through a simple Google search that one of the trustees was previously President of the National Assembly in the high risk country and had approved legislation relating to the class of business the firm specialised in. Another trustee had held several political posts including two ministerial positions. Further research established other connections between the charity and politically-exposed persons that the firm failed to identify.

73. Six firms had recently started to use commercially-available intelligence tools to assist with due diligence and verifying information provided by third parties. Interestingly, five of these firms were visited following the publication of our interim findings which suggested using them.

One firm had recently started to use an intelligence database to identify connections to politically-exposed persons and individuals against whom adverse information was known. All new third parties would be checked using this tool and the firm had run the names of all past third party payees through the database and was checking the results.

74. These six firms now routinely checked whether new and existing third parties were public officials or connected to public officials. The other firms in our sample did not satisfy us that they knew how to check for political connections. This was disappointing because, in many cases, a simple internet search would produce useful results. We were also concerned that there were some circumstances where firms appeared willing to enter into relationships with third parties whom they knew to be public officials or politically-exposed persons without taking adequate steps to ensure that payments made were not illicit.

One firm was considering using a third party to win business when they knew he had family and shareholder connections with insurance companies in a high risk country with heavy state ownership. It was therefore possible he may have been a politically-exposed person. He may also have been connected with the assured or client but this had not been investigated by the firm. In addition, the third party was resident in Switzerland, used Swiss bank accounts, and only communicated with the firm via Hotmail.

75. More worryingly, none of the firms in our sample appeared to take adequate steps to ensure that third parties were not connected with either the assured or the client.

When asked if a third party might have been connected to the client, a Managing Director of one larger firm said 'He could be his brother-in-law for all I know'.

76. One relatively simple way for firms to achieve more transparency would be to inform the assured and/or client of any third party receiving commission as a matter of course. However, we did not identify any firm in our sample which routinely appeared to do this and we identified some instances where firms appeared willing to disguise a third party's involvement in a transaction.

We saw an email between two employees of a broker firm regarding setting up a third party account which stated in bold that the third party 'do not want their name to appear on any debit/cover notes'. This should have alerted the firm to an increased risk of bribery and corruption.

3.3.4 Due diligence on business acquired from other firms

77. The commercial insurance broking sector has seen a high number of mergers and acquisitions in recent years. This means that it is – and has been – common for third party relationships to be transferred from one firm to another as business or teams are acquired.

78. Against this background, we were disappointed to find that several firms had not reviewed or conducted their own due diligence on third parties when teams or business was acquired from other firms, nor had they conducted sample checks on the quality of the acquired firm's due diligence to assess whether this was in line with their own procedures and requirements. In fact, only two firms told us that they conducted full reviews of the due diligence carried out on acquired third parties to ensure the appropriateness of the relationship.

One firm put all acquired third parties through its own due diligence process before allowing payments to them. This reduced the risk that illicit payments would be made when third party relationships had not been subject to equivalent due diligence in the past.

79. In general, there was far too heavy a reliance on the firm from which business was acquired to have carried out adequate due diligence. We would remind firms that they are responsible for all the business on their books. They cannot point to inadequacies in another firm's past due diligence on third party relationships as a defence for weaknesses in their own systems and controls. It is essential that firms understand the business case for all their third party relationships, whether they established them or acquired them. They should also consider the level of risk in their acquired business and whether their existing due diligence processes remain adequate, particularly if the new business is higher risk.

One firm had recently acquired business from another firm, which was significantly higher risk than its traditional book, mainly because of the countries involved. Despite this, no enhanced controls or due diligence were put in place and we found due diligence to be very weak across both the historical and acquired parts of the business.

80. Our review showed that most firms have significant or serious weaknesses in due diligence standards for third party relationships. Firms should consider this carefully when acquiring business from others.

3.3.5 What is a reasonable level of commission?

81. It is important that firms consider the risk that 'commission payments' to third parties could themselves be bribes or passed on by the third party to others as illicit payments for obtaining or retaining business.

82. Generally, we found the level of commission paid to third parties was not carefully considered by broker firms from an anti-bribery and corruption perspective. The main considerations were winning the business, maximising retained brokerage and incentivising third parties to win more business for them in future. This was despite the fact that many firms acknowledged they were dealing in high risk countries and classes of business.

83. Despite the drive in many firms to keep third parties' commission to a minimum, we found commission was often shared equally, or nearly equally, between firms and third parties. In most firms there was no real consideration of whether payments made to third parties were commensurate with the services they provided, the costs they were likely to incur or, most importantly, the bribery and corruption risk posed by paying relatively large amounts of commission to third parties, particularly for higher risk business.

One firm's CEO said his main consideration when deciding the level of commission for third parties was what the third party was currently receiving from, or being offered by, other firms in relation to the business they were trying to win. We did not see any evidence of bribery and corruption risk being taken into account.

84. We saw very little evidence of firms setting either risk-based commission limits or guidelines – either in absolute terms or as percentages – for different third party roles, countries or classes of business on a risk basis.

85. In addition, very few firms paid third parties, which were pure introducers, on a one-off fee basis. Therefore, many introducers received commission for the lifetime of a broker firms' relationship with the relevant client, even if the third party introducer played very little or no further role in it.

3.3.6 Confirming third parties' bank details

86. It is good practice for firms to confirm that bank accounts used by third parties to receive payments are, in fact, owned and controlled by the individual or entity for which the payment is meant. Failure to do so exposes firms to the risk that they might unwittingly make illicit payments to third parties who have not been subject to the firm's normal due diligence processes. This could happen if, for example, an approved third party with corrupt intentions provided the banking details of an individual or entity to which he wished divert an illicit payment.

87. We found that most firms received bank details from third parties via informal channels, usually email. And in some cases bank details were sent from email addresses which did not appear to be obviously connected to the third party in question, for example Hotmail addresses.

At one firm, we reviewed a file relating to a third party individual which the firm was considering using to win business in a high risk country. The file indicated that all communication with the individual, including the receipt of bank account details, was via Hotmail and there was no evidence that anyone from the firm had ever met him.

88. However, following the publication of our interim findings, several firms had revised their procedures in this area and required third parties to provide confirmation of bank account details on an official letterhead signed by two directors. However, broker firms should note this method does not mitigate the risk that a corrupt third party firm's directors could deliberately give the bank details of another party and 'confirm' them as their own.

One firm visited towards the end of our review had historically received bank details by email, including Hotmail, but since the publication of our interim findings had required confirmation of bank details on an official letterhead signed by two directors.

89. Some potentially more effective methods broker firms might wish to use to verify third party bank account details might include:

- obtaining an original bank statement from the third party showing the sort code, account number and name of account holder and having an appropriately authorised member of staff at the broker firm sign a copy to say they have seen the original; or
- requesting the third party write the broker firm a very low value cheque (eg £0.01 or $0.01) which can then be kept on file. This will show the name of the account holder, the sort code and bank account number.

90. It is good practice for firms to take similar steps should a third party's bank details change during the course of a relationship. These sorts of measures to confirm bank details should also reduce the more general payment fraud risks faced by firms.

3.3.7 Approval of third party relationships and associated due diligence

91. It is good practice for broker firms to ensure that due diligence documentation is reviewed by somebody independent of the broking department. This is because individual brokers may be inclined to take a less rigorous approach to due diligence if using a third party produces significant brokerage and has a positive effect on their personal remuneration. For more on risks arising from remuneration structures, see Section 3.7.

92. The majority of firms required approval of third party accounts from outside the broking department, usually by compliance, risk, the CEO, Chief Operating Officer or a committee comprising individuals from these areas. And a small number of firms had a risk-based approach to third party approval whereby certain members of senior management were required to sign-off high risk accounts even though they had been approved by compliance.

One firm's compliance department checked all third party due diligence carried out by the broking department and sought independent verification of the information using a range of tools. A secondary sign-off from the CEO or Chief Risk Officer was required for higher risk third party relationships.

93. However, we saw several firms where third party relationships were approved by compliance and/or other senior managers despite significant weaknesses in due diligence and a lack of understanding of the business case for the third party. It is important that individuals and committees responsible for approving third party relationships ensure they are satisfied with the underlying due diligence before approving them.

At one firm, the individual responsible for recommending approval of higher risk third party accounts did not have a formal compliance role, did not consider himself to be part of the compliance function and provided little challenge to the broking department's due diligence. He said he would sometimes see a third party's CV or annual accounts but added that he considered this to be 'overkill'. He also said that 'more often than not' the decision about whether to recommend opening a third party account 'comes down to gut feeling'. This lax approach to account approval was exacerbated as the relevant committee with ultimate responsibility for approving new third party accounts was unlikely in practice to challenge the individual's recommendations. Third party accounts were therefore opened on the basis of very little or no due diligence.

94. Despite the conflict inherent in arrangements where brokers approve due diligence on third parties they propose to use, we found no independent checking of due diligence outside the broking department occurred in some firms. This is poor practice.

3.3.8 Reviews of third party relationships

95. It is good practice for firms to review third party relationships regularly to ensure changes to their nature and risk profile are identified and are subject to appropriate approval. Firms may decide to vary the frequency of third party reviews on a risk basis so they can focus their resources on the areas of highest risk. In these circumstances, it is important that firms' risk classifications for third parties and the appropriate frequencies for review are well thought through and clearly defined. For more on risk assessment, see Section 3.2.1.

One firm had recently introduced a two-yearly standard review of third party relationships, with more frequent reviews for those which were higher risk. However, the Compliance Officer responsible for reviews had sole discretion in determining which relationships were higher risk. There was no written document setting out the factors which would make a relationship 'higher risk'. It was therefore possible that risk assessment would not be done consistently and that some higher risk accounts might not be reviewed as often as they should be.

96. We were disappointed to find that most firms had historically not conducted regular reviews of approved third party relationships. Consequently, redundant third party accounts were often 'live' on the accounting system and could have been used for fraudulent purposes including making payments to third parties which were not approved or due commission. Many firms' informal approach to due diligence meant they relied heavily on the fact that third party relationships were often longstanding, even though little or no due diligence had been conducted.

97. However, several firms we visited were now introducing regular reviews of third party relationships, particularly in light of the Aon case and our interim findings. But, even in these circumstances, some firms said they found it extremely difficult to ask long-standing third party introducers for new or updated information in relation to the role they carried out.

One firm only opened third party accounts for a maximum of one year. After this period the account would automatically be closed on the accounting system and need to be reapproved. Where commission payments were less frequent than annual, the firm approved due diligence on a transactional basis.

The importance of central records

98. It is good practice for firms to keep central records of approved third parties, underlying due diligence and evidence of periodic reviews of the relationship. It is difficult to see how firms which do not do this can adequately monitor third party relationships on a continuing basis or know when or if reviews of third party relationships are due.

One firm, which made commission payments to third party individuals in high risk countries, said they collected evidence of a third party's identity at the outset of a relationship. However, this did not appear to be kept as no third party files were maintained and the business case for using third parties was not documented.

99. Some firms did not have – or could not provide us with – a central list of all the third parties used to win business. In addition, some firms did not keep due diligence documentation in a central repository or single format and others could not routinely produce a list of payments made to third parties for a given period. It therefore took some firms several weeks to put together lists of third party payments for us and our subsequent discussions with firms indicated that they were sometimes incomplete or inaccurate.

An independent review of one firm's controls over third parties identified that approved third party introducers were not clearly labelled on its IT system. The 18 third party introducers used by the firm were put in the same category as 300 other entities including loss adjusters, brokers and surveyors. In addition, the independent review found there was no process in place for ensuring that redundant third party accounts were closed down.

3.3.9 Due diligence on third party relationships – examples of good and poor practice

Good practice

- Establishing and documenting policies with a clear definition of a 'third party' and the due diligence required when establishing and reviewing third party relationships.
- More robust due diligence on third parties which pose the greatest risk of bribery and corruption, including a detailed understanding of the business case for using them.
- Having a clear understanding of the roles clients, reinsurers, solicitors and loss adjusters play in transactions to ensure they are not carrying out higher risk activities.
- Taking reasonable steps to verify the information provided by third parties during the due diligence process.
- Using third party forms which ask relevant questions and clearly state which fields are mandatory.
- Having third party account opening forms reviewed and approved by compliance, risk or committees involved in these areas.
- Using commercially-available intelligence tools, databases and/or other research techniques such as internet search engines to check third party declarations about connections to public officials, clients or the assured.
- Routinely informing all parties involved in the insurance transaction about the involvement of third parties being paid commission.
- Ensuring current third party due diligence standards are appropriate when business is acquired that is higher risk than existing business.
- Considering the level of bribery and corruption risk posed by a third party when agreeing commission levels.
- Setting commission limits or guidelines which take into account risk factors related to the role of the third party, the country involved and the class of business.
- Paying commission to third parties on a one-off fee basis where their role is pure introduction.

- Taking reasonable steps to ensure that bank accounts used by third parties to receive payments are, in fact, controlled by the third party for which the payment is meant. For example, broker firms might wish to see the third party's bank statement or have the third party write them a low value cheque.
- Higher or extra levels of approval for high risk third party relationships.
- Regularly reviewing third party relationships to identify the nature and risk profile of third party relationships.
- Maintaining accurate central records of approved third parties, the due diligence conducted on the relationship and evidence of periodic reviews.

Poor practice

- Failing to carry out or document due diligence on third party relationships.
- Relying heavily on the informal 'market view' of the integrity of third parties as due diligence.
- Relying on the longstanding nature of third party relationships when no due diligence has ever been carried out.
- Carrying out only very basic identity checks as due diligence on higher risk third parties.
- Asking third parties to fill in account opening forms which are not relevant to them (e.g. individuals filling in forms aimed at corporate entities).
- Accepting vague explanations of the business case for using third parties.
- Approvers of third party relationships working within the broking department or being too close to it to provide adequate challenge.
- Accepting instructions from third parties to pay commission to other individuals or entities that have not been subject to due diligence.
- Assuming that third party relationships acquired from other firms have been subject to adequate due diligence.
- Paying high levels of commission to third parties used to obtain or retain higher risk business, especially if their only role is to introduce the business.
- Receiving bank details from third parties via informal channels such as email, particularly if email addresses are from webmail (e.g. Hotmail) accounts or do not appear to be obviously connected to the third party.
- Leaving redundant third party accounts 'live' on the accounting systems as a result of failure to review third party relationships regularly.

- Being unable to produce a list of approved third parties, associated due diligence and details of payments made to them.

3.4 Payment controls

3.4.1 Insurance broking accounts

100. Systems and controls over payments to third parties form a key line of defence in preventing bribery and corruption. But however effective they are in themselves, they will be ineffective if the underlying due diligence on third party relationships is of poor quality.

101. We found the systems and controls around payments to third parties appeared generally adequate, with clear, risk-based payment authorisation procedures usually in place and payments to third parties prohibited unless there was an approved, live third party account on the system. We found that there were sound systems and controls in place at ten firms we visited, and there was only one firm with major shortcomings.

102. Against this, our confidence in the robustness of the payment controls was often tempered by the weaknesses in third party due diligence described in Section 3.3. Because of these weaknesses in due diligence, payments were often made to third parties without the firm clearly understanding or verifying the business rationale.

103. Advance commission payments should be considered as higher risk as they could be bribes to win business or used to facilitate them. We found that advance commission payments were generally not made by the firms we visited. However, one large firm had paid commission to new third parties in advance of premiums being received or due diligence completed, even though this was not its normal practice. In another case, a smaller firm appeared to have paid commission in advance in breach of its own procedures.

One firm's policy was not to make payments to third parties who are individuals, yet our review of their third party payments schedule showed they had made such payments in the last two years.

104. Hardly any firms monitored payments over time to identify unusual payments to third parties, despite the fact that most firms could produce schedules of third party payments without difficulty. We consider it is good practice for firms to conduct this type of review. During our visits we discussed schedules of third party payments made over the last two years, and several firms commented that regularly reviewing payments in this way would be a valuable exercise.

At one firm, the Compliance Officer said regular payments of small amounts would raise concerns about bribery and corruption. We highlighted a number of third party payments made by the firm to an individual which fell into this category. The Compliance Officer appeared concerned by these payments and confirmed he had never reviewed payments in this way before.

3.4.2 Accounts payable

105. Firms should be aware of the risk that Accounts Payable can be used to make payments or inducements to third parties who may not have been subject to due diligence and appropriately approved. Examples of payments or inducements that can be made to third parties via Accounts Payable include excessive entertainment, gifts and hospitality, cash payments and payments of lifestyle-related bills such as travel or school fees. Firms should therefore ensure that they have adequate systems and controls in place to mitigate this risk.

106. It is good practice for firms to limit third party payments from Accounts Payable to reimbursements of genuine business-related costs or reasonable entertainment which is unlikely to be construed as an inducement and ensure that the reasons for payment are clearly documented and approved.

As part of routine supervision, we found that a broker firm's Chairman, based overseas, operated through a corporate entity in an offshore financial centre and introduced high-risk business to the broker firm. The broker firm paid advance travel expenses of around £200,000 annually to the offshore corporate entity and did not require any proof of expenditure in return. In addition, the annual travel budget for the corporate entity was determined based on the previous year with few questions asked by the broker firm. There is a risk in these circumstances that some or all advance travel expenses can be used to make illicit payments to win business.

107. Although we did not carry out any practical testing of how Accounts Payable is used, we discussed relevant procedures with accounting staff to understand the quality and effectiveness of controls to ensure the accuracy and transparency of payments.

108. Generally, systems and controls over staff expenses and accounts payable appeared to be adequate, but some firms had no formal limits on staff entertaining, expenditure or travel. In general, we found that although the controls appeared to be strong, this was mainly to ensure value for money or to cut costs, rather than to mitigate bribery and corruption risk.

Each month, one smaller firm's Finance Director conducted an in-depth review of the travel expenses of one individual over the past twelve months.

109. All firms visited required staff to produce receipts for expenditure and expenses to be signed off by an authorised person. In many cases other evidence was sought if a receipt was genuinely lost or mislaid. However, some firms told us that large cash advances were sometimes given to staff for travelling in higher risk countries where they said credit cards were not readily accepted. Firms should consider carefully the risk of allowing staff to travel to high risk countries with large amounts of cash.

One firm advanced significant sums of cash to staff visiting a very high risk country where, it said, credit cards were not accepted. They said hotels in this country cost

$600-$1000 per night, meaning that large sums of cash were needed on these trips. Our subsequent research found that good quality business hotels could be booked in that country in advance through well-known, on-line travel agents. Therefore, there was no need for this firm's staff to take large amounts of cash on their visits.

110. Most firms visited had a Gifts Register with clear associated procedures although, in some cases, they had only recently been introduced. We noted that one firm's thresholds for recording of gifts and entertainment on the Register included £500 for entertainment and £300 for cash. We regard it as poor practice in all circumstances for firms either to give or receive gifts of cash.

3.4.3 Payment controls – examples of good and poor practice

Good practice

- Ensuring adequate due diligence on and approval of third party relationships before payments are made to the third party.
- Risk-based approval procedures for payments and a clear understanding of the reason for all payments.
- Checking third party payments individually prior to approval, to ensure consistency with the business case for that account.
- Regular and thorough monitoring of third party payments to check, for example, whether a payment is unusual in the context of previous similar payments.
- A healthily sceptical approach to approving third party payments.
- Adequate due diligence on new suppliers being added to the Accounts Payable system.
- Clear limits on staff expenditure, which are fully documented, communicated to staff and enforced.
- Limiting third party payments from Accounts Payable to reimbursements of genuine business-related costs or reasonable entertainment.
- Ensuring the reasons for third party payments via Accounts Payable are clearly documented and appropriately approved.
- The facility to produce accurate MI to assist effective payment monitoring.

Poor practice

- Failing to check whether third parties to whom payments are due have been subject to appropriate due diligence and approval.
- Failing to produce regular third party payment schedules for review.

- Failing to check thoroughly the nature, reasonableness and appropriateness of gifts and hospitality.
- No absolute limits on different types of expenditure, combined with inadequate scrutiny during the approvals process.
- The giving or receipt of cash gifts.

3.5 Staff recruitment and vetting

111. A good standard of staff recruitment and vetting is important if firms are to reduce the risk of employing staff who may be easily persuaded or willing to engage in corrupt practices. We have examined recruitment and vetting standards in the financial services industry during previous thematic reviews, most notably our 2008 report, *Data Security in Financial Services*,[6] and our soon-to-be published *Small Firms Financial Crime Review*. We did so again as part of this work.

112. We expect firms to take a risk based approach to recruitment and vetting, which takes into account the financial crime risks they face. In the context of anti-bribery and corruption, firms should consider enhanced vetting of staff in higher risk positions. These are likely to include:

- brokers handling higher risk business involving third parties;
- accounts staff responsible for processing payments to third parties; and
- those responsible for approving or reviewing third party relationships.

113. Firms should also consider, depending on how they are organised and responsibilities apportioned, whether there are other individuals whom it would be appropriate to subject to enhanced vetting.

114. In general, we found that the vetting of staff in many broker firms appeared to be weak compared with other financial services sectors. There was a heavier than usual reliance on informal factors such as market gossip, referrals and acquaintances, and many firms' pre-employment checks were limited to references (even though most firms appeared to view them to be of little use). Most firms appeared to target their staff, particularly brokers, known to them informally in the market and, as a result of this loose acquaintance, chose not to carry out formal checks of criminal records or financial soundness.

115. Only seven of the 17 firms visited conducted criminal record checks, although some others asked job applicants to disclose criminal convictions. Criminal record checks were focused mainly on approved persons; only three firms checked higher risk non-FSA-approved individuals but three others were considering this.

6 See: http://www.fsa.gov.uk/pubs/other/data_security.pdf

One firm had historically carried out criminal record checks only for senior staff but had recently revised their procedures to include all new joiners. They were also considering carrying out criminal record checks on existing staff. One of the factors leading to this change in approach was that they recruited a member of broking staff through an agency and had later discovered he had a criminal conviction.

116. It is good practice for firms to check individuals' financial soundness so they can identify staff members who might be more susceptible to committing or becoming involved in corrupt practices or other financial crime. We found that a similar number of firms carried out credit checks compared with criminal record checks, although few firms conducted both. And, in most cases, seniority rather than risk appeared to be the key factor in determining whether to undertake checks on an individual.

117. A minority of firms, when recruiting staff who had previously worked in other regulated firms, checked with relevant regulators to ensure the individual had no history of discipline or misconduct. Another small number of firms which had recently introduced commercially-available intelligence tools for the purposes of third party due diligence had begun using them as a vetting tool in their recruitment process. However, we found no firms in our sample were making use of the CIFAS staff fraud database.[7]

118. It is good practice for firms to take a risk-based approach to dealing with adverse information raised by vetting checks, taking into account their seriousness, relevance and the individual's role or proposed role. In some cases, firms may decide that adverse findings against an individual are so serious that they should not be employed or should have their employment terminated; in others, the firm might decide the risk posed is not as serious but choose to restrict the individual's responsibilities to lower risk areas or subject them to enhanced management oversight. There may even be cases where adverse findings against an individual are considered not to be serious or relevant in the context of the individual's role and no further action is taken.

One firm conducted criminal record and credit checks for approved persons, appointed representatives and introducer appointed representatives. They were considering extending this checking to higher risk staff and repeating checks every three years. HR and the Chief Operating Officer discussed adverse information revealed by vetting checks on a case-by-case basis to ensure an appropriate response.

119. We found that very few firms employed temporary or contract staff in positions we would consider as higher risk from a bribery and corruption perspective. However, where firms use employment agencies to recruit staff, particularly for higher risk positions, it is good practice for them to have a clear understanding of the checks conducted by agencies on prospective staff. They should also consider conducting periodic checks to ensure that agencies are complying with agreed vetting standards.

7 The CIFAS Staff Fraud Database is used by CIFAS Members specifically for staff vetting and security screening purposes. CIFAS members use the Staff Fraud Database to file data about their staff fraud cases and access staff fraud records filed by other CIFAS Members. For more information, visit: http://www.cifas.org.uk/default.asp?edit_id=718-87

120. It is important for firms to ensure that, just because a member of staff is employed on a temporary basis, they are not subject to less rigorous vetting than permanent staff in the same or similar roles. The risk of bribery and corruption does not decrease when a temporary member of staff or contractor handles higher risk business so nor should the standard of vetting.

121. Only two firms repeated any form of vetting during employment. In both cases, these were credit checks with one firm conducting them annually for all staff and another carrying out random checks on finance staff every two to three years. Most firms had no formal process for identifying a change in an existing employee's financial soundness which might make them more vulnerable to becoming involved in or committing corrupt practices.

3.5.1 Staff recruitment and vetting – examples of good and poor practice

Good practice

- Vetting staff on a risk-based approach, taking into account financial crime risk.
- Enhanced vetting – including checks of credit records, criminal records, financial sanctions lists, commercially-available intelligence databases and the CIFAS Staff Fraud Database – for staff in roles with higher bribery and corruption risk.
- A risk-based approach to dealing with adverse information raised by vetting checks, taking into account its seriousness and relevance in the context of the individual's role or proposed role.
- Where employment agencies are used to recruit staff in higher risk positions, having a clear understanding of the checks they carry out on prospective staff.
- Conducting periodic checks to ensure agencies are complying with agreed vetting standards.
- A formal process for identifying changes in existing employees' financial soundness which might make them more vulnerable to becoming involved in or committing corrupt practices.

Poor practice

- Relying entirely on an individual's market reputation or market gossip as the basis for recruiting staff.
- Carrying out enhanced vetting only for senior staff when more junior staff are working in positions where they could be exposed to bribery or corruption.
- Failing to consider on a continuing basis whether staff in higher risk positions are becoming vulnerable to committing fraud or being coerced by criminals.

- Relying on contracts with employment agencies covering staff vetting standards without checking periodically that the agency is adhering to them.
- Temporary or contract staff receiving less rigorous vetting than permanently employed colleagues carrying out similar roles.

3.6 Training and awareness

122. It is essential for firms to have adequate policies and procedures to mitigate the risks of bribery and corruption. But it is equally important that relevant staff are given the right training so they understand the risks they face, act in a way the firm expects and avoid breaching company policy, regulatory requirements or the law. There is no point in firms having sensible, documented policies and procedures if staff do not know how to access them or understand what the policies require.

123. We were therefore very disappointed to find that only two of the seventeen firms visited provided adequate staff training on anti-bribery and corruption. The other firms had various weaknesses in their training and awareness programmes.

One firm had no written procedures or training on third party due diligence, and very little senior management involvement in anti-bribery and corruption issues. Almost all responsibility for anti-bribery and corruption had been devolved to the Compliance Officer who lacked support.

124. Most firms required staff to take, and in some cases pass a test on, 'financial crime' training (which was usually computer-based or a presentation from the compliance department). However, there was usually very little or no specific material within these training programmes covering anti-bribery and corruption, even for staff in higher risk positions.

125. We also found that most firms provided training through a standard package. There were no enhanced modules for staff in critical, higher-risk roles, such as producing brokers, compliance or accounts. In addition, there were very few examples of training that gave practical examples of how to comply with policies and procedures, situations which might increase bribery and corruption risk and appropriate due diligence on third party relationships. Instead, it tended to focus on legislative and regulatory requirements, which front-line staff would find difficult to understand without further guidance. However, some firms said they were considering introducing more specific training for certain, higher risk staff.

Several firms did not provide training on anti-bribery and corruption as they said the correct payment procedures had to be followed in order for third party payments to be made. However, many of these firms had serious weaknesses in third party due diligence which undermined payment controls. These weaknesses in due diligence standards were at least partially caused by a lack of good quality training for relevant staff.

126. Where training was provided, there was often no testing to ensure staff understood it, and compliance and other staff responsible for training staff on financial crime had generally not received any specialist training on anti-bribery and corruption themselves. Our visits also confirmed a poor understanding of financial crime risk among senior managers and other relevant staff in some firms. This lack of specialist knowledge among staff responsible for anti-bribery and corruption at many firms is likely to be a major contributory factor to the poor quality of anti-bribery and corruption systems and controls in broker firms.

In one firm, the Compliance Manager in particular demonstrated a poor understanding of the distinctions between politically-exposed persons, financial sanctions, anti-money laundering and anti-bribery and corruption. At another, the person responsible for bribery and corruption risk did not understand the risk of using a third party to introduce business and we spent around 20 minutes explaining this to him.

127. It is important for firms to be able to demonstrate that staff understand the training they have been given. This is not only for regulatory reasons; it also allows firms to assess the quality and adequacy of their training. For example, if a few staff fail a test, this might highlight extra training needs; if large numbers of staff fail, this might indicate that the training is unclear and needs to be overhauled; and if everybody passes with full marks, the training might be too basic.

One firm, which used a professional consultant to help improve anti-bribery and corruption systems and controls, introduced compulsory financial crime training for new and existing staff. This included an on-line module covering anti-bribery and corruption with a test and supporting seminar. There were also clear plans for annual refresher courses.

128. Only four firms had arrangements in place for refresher training although some others said they were considering this. It is good practice for firms to repeat training periodically and ensure training material is kept up-to-date, otherwise staff may be unaware of the latest requirements and standards (both internal and external). Keeping training material up-to-date is important as staff are likely to find carrying out the same training year after year boring and this could ultimately cause them to take less of an interest in anti-bribery and corruption – the exact opposite of the objective of training staff.

3.6.1 Training and awareness – examples of good and poor practice

Good practice

- Providing good quality, standard training on anti-bribery and corruption for all staff.
- Additional anti-bribery and corruption training for staff in higher risk positions.

- Ensuring staff responsible for training others have adequate training themselves.
- Ensuring training covers practical examples of risk and how to comply with policies.
- Testing staff understanding and using the results to assess individual training needs and the overall quality of the training.
- Maintaining staff records setting out what training was completed and when.
- Providing and maintaining refresher training.

Poor practice

- Failing to provide training on anti-bribery and corruption, especially to staff in higher risk positions.
- Training staff on legislative and regulatory requirements but failing to provide practical examples of how to comply with them.
- Failing to ensure anti-bribery and corruption policies and procedures are easily accessible to staff.
- Neglecting the need for appropriate staff training in the belief that robust payment controls are sufficient to combat anti-bribery and corruption.

3.7 Risks arising from remuneration structures

129. The appropriateness of remuneration structures and the ways in which they affect risk have been a matter of much political and regulatory debate since the onset of the current financial crisis. We became the first regulator in the world to set rules concerning remuneration structures when, in August 2009, we introduced a Remuneration Code (the Code) requiring large UK banks, building societies and broker dealers to establish, implement and maintain remuneration policies consistent with effective risk management. This Code came into effect in January 2010.[8]

130. When the Code was launched, our Chief Executive, Hector Sants, said the aim was to ensure that 'remuneration policies [are] consistent with, and promote, effective risk management.' Although the Code does not apply to insurance brokers, we regard it as good practice for broker firms to consider whether their remuneration structures give rise to increased risk of bribery and corruption and whether they should introduce arrangements to reduce significant risks.

131. However, we found little evidence that broker firms had considered specifically whether staff, particularly producing brokers dealing with or using third parties, might be influenced to engage in, or facilitate, bribery when the winning of business would benefit their personal remuneration.

8 See: http://www.fsa.gov.uk/pages/Library/Communication/PR/2009/108.shtml

One firm had four staff – the CEO, Chairman and two other executive directors, all of whom were heavily involved in production – whose bonuses comprised a share of the firm's pre-tax profits and were usually larger than their annual salary. Two of these staff also sat on the Committee responsible for approving third party relationships. This kind of remuneration structure increases the risk that those approving third party relationships might overlook inadequacies in due diligence if they would benefit financially from the business third parties introduce.

132. Worryingly, a significant number of firms visited had bonus schemes for producing brokers which focused entirely on the income or profit they generated and, in some cases, there was a direct formulaic link. It is our view that remuneration structures of this kind could encourage risk-taking and negligence and increase the risk of bribery and corruption, particularly where producing brokers use third parties to win business. This underlines the need for effective due diligence on third party relationships by staff independent of the producing department.

One firm had a special bonus scheme directly linked to the generation of as much brokerage as possible. In order to trigger the bonus, producing brokers had to generate income of at least 2 times their salary. They would then receive a 10% share of the first £200,000 they produced above that threshold; 15% for amounts between £200,000 and £500,000; and 20% for amounts over £500,000.

3.7.1 Remuneration structures likely to reduce risk

'Balanced scorecards'

133. Several firms had introduced reward structures where several factors, including those linked to audit issues and general good compliance practice, would be taken into account when determining the level of an individual's bonus. This kind of reward structure is often referred to by HR staff as a 'balanced scorecard'. Although these balanced scorecard structures did not appear to have been introduced specifically to minimise the risk of bribery and corruption, it is likely that they would encourage a more responsible, balanced approach from producing brokers who, historically, might have been more aggressively focussed on generating income.

Following an overhaul of their bonus system, one firm was experiencing difficulties in persuading a small number of staff to move off their income-based deals. As an incentive for them to change their contractual remuneration arrangements and move to the new bonus scheme, these staff were not allowed to buy shares in the company until they relinquished their income-based remuneration arrangements.

Deferral and clawback of bonuses

134. We were encouraged – and pleasantly surprised – to find that four firms had bonus schemes whereby a proportion of individuals' bonuses were deferred and, in some cases, subject to 'clawback'.[9] Examples of how some firms structured their deferred bonus schemes are set out in the box below.[10]

Firm A: *60% of bonus paid up-front with the deferred 40% paid in instalments of 10% each year for four years.*

Firm B: *For bonuses due this year, 80% paid up-front, with 20% paid one year later; for bonuses due in subsequent years, 70% paid up-front with 30% paid one year later.*

Firm C: *25% of bonus paid up-front with the deferred 75% paid in instalments of 25% each year for three years.*

135. As with the introduction of balanced scorecards, the use of bonus deferral and clawback by broker firms did not appear to have been specifically driven by anti-bribery and corruption priorities. Instead, many firms had introduced it to discourage staff from moving to other firms. However, we judge that the incentives for producing brokers to cut corners or take risks when dealing with third parties will be reduced by deferral and claw-back, regardless of the underlying motives for their use.

3.7.2 Risks arising from remuneration structures – examples of good and poor practice

Good practice

- Assessing whether remuneration structures give rise to increased risk of bribery and corruption.
- Determining individual bonus awards on the basis of several factors, including a good standard of compliance, not just the amount of income generated.
- Deferral and clawback provisions for bonuses paid to staff in higher risk positions.

Poor practice

- Bonus structures for staff in higher risk positions which are directly linked (e.g. by a formula) solely to the amount of income or profit they produce, particularly when bonuses form a major part, or the majority, of total remuneration.

9 'Clawback' arrangements usually allow firms to withhold the deferred element of a bonus if certain objectives or targets are not achieved by the employee.

10 To note, the FSA's Remuneration Code states that a significant proportion of any bonus should be deferred, with the deferred element vesting no faster than three years.

3.8 Incident reporting

3.8.1 Suspicious Activity Reports

136. Although broker firms are not subject to the Money Laundering Regulations, all firms visited had appointed someone to carry out a role similar to a Money Laundering Reporting Officer (MLRO). However, only four firms visited had ever submitted a Suspicious Activity Report (SAR) and only one had ever made a SAR related to bribery and corruption. This was despite the fact that, during our review, we identified many examples of high risk third party relationships that did not appear to have a clear business case.

One firm visited, which had never submitted a SAR, was unaware of the correct procedure for the reporting of suspicions, and thought SARs should be sent to the FSA rather than SOCA.

137. In addition, several firms had weaknesses in their reporting procedures, for example not having an internal form for reporting suspicions to the 'MLRO' or not having clear procedures on the internal reporting of suspicions.

One firm had never submitted a SAR but when we visited them we noticed several third party relationships which did not appear to have a clear business case. The firm conducted follow up work on third party relationships and made SARs as a result.

138. Detailed practical guidance on the steps firms can take to meet their legal and regulatory obligations relating to anti-money laundering is available from the Joint Money Laundering Steering Group (JMLSG), a body made up of trade associations from across the industry. Although the JMLSG Guidance is addressed to firms in the industry sectors represented by its member bodies, other financial services firms – such as commercial insurance brokers – are encouraged to have regard to this guidance. Chapter 6 of the JMLSG Guidance[11] covers suspicious activity reporting.

One firm, which had never made a SAR, told us about a 'recent near miss' involving an instruction from a state insurance company in high risk country A to make a payment to a firm in high risk country B. The broker firm's investigations led to a suspicion that a director of the firm in Country B might be an employee of the state insurance company in Country A. The broker firm's Compliance Officer, who also acted as MLRO, said this was probably an issue he should have reported.

3.8.2 Whistleblowing

139. Whistleblowing procedures allow staff to inform senior management about misconduct or other concerns they encounter during their work. We examined whether firms had whistleblowing policies and procedures in place and how well they were used as corrupt practice within a firm could highlighted to senior management by whistleblowers.

11 See: http://www.jmlsg.org.uk/content/1/c6/01/14/56/Part_I_-_HMT_approved.pdf

140. A number of firms had a formal whistleblowing procedure, but in most cases this had never been used. Although it is difficult to judge the reasons for this, we noticed that most firms had made little effort to make staff aware of whistleblowing procedures. Some small firms expressed concerns about the wisdom of having an in-house whistleblowing facility when the size of the firm meant it would be difficult to submit information anonymously.

One small firm had outsourced its whistleblowing facility to an external agency. This afforded whistleblowers a level of confidentiality that would have been difficult to achieve in-house.

141. Should firms' staff feel they cannot blow the whistle internally, for example because senior management might be involved in misconduct, we run an anonymous whistleblowing line for staff in regulated firms. Our whistleblowing line's telephone number is 020 7066 9200 or you can email whistle@fsa.gov.uk. In addition, the UK charity, 'Public Concern at Work', offers free advice to people with whistleblowing dilemmas and professional support to organisations who need advice on how to set up whistleblowing facilities.[12]

3.8.3 Incident reporting and management – examples of good and poor practice

Good practice

- Clear procedures for whistleblowing and the reporting of suspicions which are communicated to staff.
- The appointment of a senior manager to oversee the whistleblowing process and act as a point of contact if an individual has concerns about their line management.
- Respect for the confidentiality of workers who raise concerns.
- Internal and external suspicious activity reporting procedures in line with the Joint Money Laundering Steering Group Guidance.
- Keeping records or copies of internal suspicion reports which are not forwarded as SARs for future reference and possible trend analysis.
- Financial crime training covers whistleblowing procedures and how to report suspicious activity.

Poor practice

- Failing to report suspicious activity relating to bribery and corruption.
- No clear internal procedure for whistleblowing or reporting suspicions.

12 http://www.pcaw.co.uk

- No alternative reporting routes for staff wishing to make a whistleblowing disclosure about their line management or senior managers.
- A lack of training and awareness in relation to whistleblowing the reporting of suspicious activity.

3.9 The role of compliance and internal audit

142. Firms' compliance and internal audit departments should form key lines of defence in the fight against bribery and corruption. It is good practice for their work schedules to include assurance work on the adequacy of underlying due diligence on third party relationships, as well as checks to ensure appropriate approval is sought to establish and maintain relationships and that there are good business cases for making third party payments.

143. However, we found that compliance and internal audit often only considered whether the proper processes had been followed when establishing the relationships (e.g. that an appropriately authorised person in the firm had approved it). Very few firms' compliance and/or audit functions considered the adequacy of underlying due diligence or the rationale for third party payments.

144. Some firms' compliance and audit functions had never examined bribery and corruption or third party payment risk. Others had not carried out any routine, proactive work on anti-bribery and corruption beyond responding, in many cases inadequately, to external events such as the Thomas Huertas letter and the Aon case. Where routine compliance and internal audit monitoring took place, we generally found that there was not a risk-based approach to either their checking or the way anti-bribery and corruption systems and controls were devised and implemented. And, in some cases, compliance were involved in the approval process for new third party accounts but had either approved them without ensuring adequate due diligence had been carried out or were working without formal procedures.

At one firm, nearly all the third party files reviewed did not demonstrate a clear business case for their use. Due diligence forms were either not present or not completed properly, but compliance nevertheless signed them off.

145. We also found that compliance and internal audit staff generally completed no more than standard financial crime training, so their knowledge was patchy considering their important roles. However, some had attended occasional seminars and presentations by trade bodies and lawyers following the Aon case. We would reiterate that it is very important that compliance and/or internal audit staff have a very good knowledge of anti-bribery and corruption. This is because, in many firms, compliance particularly help to train staff and both functions have important roles to play on anti-bribery and corruption.

146. Several firms were too small to have an internal audit function. Of those that did, only three had carried out significant work concerning anti-bribery and corruption. At one of them, internal audit reviews included reconciling third party payment records against details held centrally and checking a sample of third party payments for adequate due diligence, compliance records and Terms of Business Agreements. Another firm used an outsourced internal auditor to carry out a detailed third party payments review.

147. There was a lack of independent oversight in some firms where compliance was responsible for approving third party relationships and/or payments, and compliance checking. In these cases, they were effectively checking their own work. However, some firms used internal audit or outsourced checking by independent parties to ensure compliance's operational role in approving third party relationships and payments was being carried out properly. Generally, we found that internal audit assurance work tended to be of a more independent nature than that carried out by compliance. This was because internal audit usually had no involvement in the third party accounts or payments approvals processes.

One small firm's Compliance Manager was responsible for approving new third parties and compliance monitoring of third party accounts. They recognised both the key person risk and potential conflict of interest inherent in these arrangements and were recruiting a second compliance person so they could separate the approval and compliance monitoring roles in relation to third parties.

3.9.1 Compliance and internal audit – examples of good and poor practice

Good practice

- Compliance and internal audit staff receiving specialist training to achieve a very good knowledge of the bribery and corruption risks.
- Effective compliance monitoring and internal audit reviews which challenge not only whether processes to mitigate bribery and corruption have been followed but also the effectiveness of the processes themselves.
- Independent checking of compliance's operational role in approving third party relationships and accounts, where relevant.
- Routine compliance and/or internal audit checks of higher risk third party payments to ensure there is appropriate supporting documentation and adequate justification to pay.

Poor practice

- Failing to carry out compliance or internal audit work on anti-bribery and corruption.
- Compliance, in effect, signing off their own work, by approving new third party accounts and carrying out compliance monitoring on the same accounts.
- Compliance and internal audit not recognising or acting on the need for a risk-based approach.

4. Consolidated examples of good and poor practice

Anti-bribery and corruption – consolidated examples of good and poor practice	
Examples of good practice	**Examples of poor practice**
Governance and Management Information	
• Clear, documented responsibility for anti-bribery and corruption apportioned to either a single senior manager or a committee with appropriate Terms of Reference and senior management membership, reporting ultimately to the Board. • Good Board level and senior management understanding of the bribery and corruption risks faced by the firm, the materiality to their business and how to apply a risk-based approach to anti-bribery and corruption work. • Swift and effective senior management-led response to significant bribery and corruption events, which highlight potential areas for improvement in systems and controls. • Regular MI to the Board and other relevant senior management forums. • MI includes information about third parties including (but not limited to) new third party accounts, their risk classification, higher risk third party payments for the preceding period, changes to third party bank account details and unusually high commission paid to third parties.	• Failing to allocate official responsibility for anti-bribery and corruption to a single senior manager or appropriately formed committee. • A lack of awareness and/or engagement in anti-bribery and corruption at senior management or Board level. • Little or no MI sent to the Board about higher risk third party relationships or payments. • Failing to include details of wider issues, such as new legislation or regulatory developments in MI. • IT systems unable to produce the necessary MI.

Anti-bribery and corruption – consolidated examples of good and poor practice

Examples of good practice	Examples of poor practice
• MI submitted to the Board ensures they are adequately informed of any external developments relevant to bribery and corruption. • Actions taken or proposed in response to issues highlighted by MI are minuted and acted on appropriately.	
Risk assessment and responses to significant bribery and corruption events	
• Regular assessments of bribery and corruption risks with a specific senior person responsible for ensuring this is done, taking into account the country and class of business involved as well as other relevant factors. • More robust due diligence on and monitoring of higher risk third party relationships. • Thorough reviews and gap analyses of systems and controls against relevant external events, with strong senior management involvement or sponsorship. • Ensuring review teams have sufficient knowledge of relevant issues and supplementing this with external expertise where necessary. • Establishing clear plans to implement improvements arising from reviews, including updating policies, procedures and staff training.	• Failing to consider the bribery and corruption risks posed by third parties used to win business. • Failing to allocate formal responsibility for anti-bribery and corruption risk assessments. • A ‘one size fits all’ approach to third party due diligence. • Failing to respond to external events which may draw attention to weaknesses in systems and controls. • Taking too long to implement changes to systems and controls after analysing external events. • Failure to bolster insufficient in-house knowledge or resource with external expertise. • Failure to report inappropriate payments to SOCA and a lack of openness in dealing with us concerning any material issues identified.

Anti-bribery and corruption – consolidated examples of good and poor practice	
Examples of good practice	**Examples of poor practice**
Risk assessment and responses to significant bribery and corruption events	
• Adequate and prompt reporting to SOCA and us of any inappropriate payments identified during business practice review.	
Due diligence on third party relationships	
• Establishing and documenting policies with a clear definition of a 'third party' and the due diligence required when establishing and reviewing third party relationships. • More robust due diligence on third parties which pose the greatest risk of bribery and corruption, including a detailed understanding of the business case for using them. • Having a clear understanding of the roles clients, reinsurers, solicitors and loss adjusters play in transactions to ensure they are not carrying out higher risk activities. • Taking reasonable steps to verify the information provided by third parties during the due diligence process. • Using third party forms which ask relevant questions and clearly state which fields are mandatory. • Having third party account opening forms reviewed and approved by compliance, risk or committees involving these areas.	• Failing to carry out or document due diligence on third party relationships. • Relying heavily on the informal 'market view' of the integrity of third parties as due diligence. • Relying on the fact that third party relationships are longstanding when no due diligence has ever been carried out. • Carrying out only very basic identity checks as due diligence on higher risk third parties. • Asking third parties to fill in account opening forms which are not relevant to them (e.g. individuals filling in forms aimed at corporate entities). • Accepting vague explanations of the business case for using third parties. • Approvers of third party relationships working within the broking department or being too close to it to provide adquate challenge.

Anti-bribery and corruption – consolidated examples of good and poor practice

Examples of good practice	Examples of poor practice
Due diligence on third party relationships	
• Using commercially-available intelligence tools, databases and/or other research techniques such as internet search engines to check third party declarations about connections to public officials, clients or the assured. • Routinely informing all parties involved in the insurance transaction about the involvement of third parties being paid commission. • Ensuring current third party due diligence standards are appropriate when business is acquired that is higher risk than existing business. • Considering the level of bribery and corruption risk posed by a third party when agreeing the level of commission. • Setting commission limits or guidelines which take into account risk factors related to the role of the third party, the country involved and the class of business. • Paying commission to third parties on a one-off fee basis where there role is pure introduction. • Taking reasonable steps to ensure that bank accounts used by third parties to receive payments are, in fact, controlled by the third party for which the payment is meant. For example, broker firms might wish to see the third party's bank statement or have the third party write them a low value cheque.	• Accepting instructions from third parties to pay commission to other individuals or entities which have not been subject to due diligence. • Assuming that third party relationships acquired from other firms have been subject to adequate due diligence. • Paying high levels of commission to third parties used to obtain or retain higher risk business, especially if their only role is to introduce the business. • Receiving bank details from third parties via informal channels such as email, particularly if email addresses are from webmail (e.g. Hotmail) accounts or do not appear to be obviously connected to the third party. • Leaving redundant third party accounts 'live' on the accounting systems because third party relationships have not been regularly reviewed. • Being unable to produce a list of approved third parties, associated due diligence and details of payments made to them.

Anti-bribery and corruption – consolidated examples of good and poor practice

Examples of good practice	Examples of poor practice
Due diligence on third party relationships	
• Higher or extra levels of approval for high risk third party relationships. • Regularly reviewing third party relationships to identify the nature and risk profile of third party relationships. • Maintaining accurate central records of approved third parties, the due diligence conducted on the relationship and evidence of periodic reviews.	
Payment controls	
• Ensuring adequate due diligence and approval of third party relationships before payments are made to the third party. • Risk-based approval procedures for payments and a clear understanding of why payments are made. • Checking third party payments individually prior to approval, to ensure consistency with the business case for that account. • Regular and thorough monitoring of third party payments to check, for example, whether a payment is unusual in the context of previous similar payments. • A healthily sceptical approach to approving third party payments.	• Failing to check whether third parties to whom payments are due have been subject to appropriate due diligence and approval. • The inability to produce regular third party payment schedules for review. • Failing to check thoroughly the nature, reasonableness and appropriateness of gifts and hospitality. • No absolute limits on different types of expenditure, combined with inadequate scrutiny during the approvals process. • The giving or receipt of cash gifts.

Anti-bribery and corruption – consolidated examples of good and poor practice

Examples of good practice	Examples of poor practice
Payment controls	
• Adequate due diligence on new suppliers being added to the Accounts Payable system. • Clear limits on staff expenditure, which are fully documented, communicated to staff and enforced. • Limiting third party payments from Accounts Payable to reimbursements of genuine business-related costs or reasonable entertainment. • Ensuring the reasons for third party payments via Accounts Payable are clearly documented and appropriately approved. • The facility to produce accurate MI to facilitate effective payment monitoring.	
Staff recruitment and vetting	
• Vetting staff on a risk-based approach, taking into account financial crime risk. • Enhanced vetting – including checks of credit records, criminal records, financial sanctions lists, commercially-available intelligence databases and the CIFAS Staff Fraud Database – for staff in roles with higher bribery and corruption risk.	• Relying entirely on an individual's market reputation or market gossip as the basis for recruiting staff. • Carrying out enhanced vetting only for senior staff when more junior staff are working in positions where they could be exposed to bribery or corruption issues.

Anti-bribery and corruption – consolidated examples of good and poor practice

Examples of good practice	Examples of poor practice
Staff recruitment and vetting	
• A risk-based approach to dealing with adverse information raised by vetting checks, taking into account its seriousness and relevance in the context of the individual's role or proposed role. • Where employment agencies are used to recruit staff in higher risk positions, having a clear understanding of the checks they carry out on prospective staff. • Conducting periodic checks to ensure that agencies are complying with agreed vetting standards. • A formal process for identifying changes in existing employees' financial soundness which might make them more vulnerable to becoming involved in or committing corrupt practices.	• Failing to consider on a continuing basis whether staff in higher risk positions are becoming vulnerable to committing fraud or being coerced by criminals. • Relying on contracts with employment agencies covering staff vetting standards without checking periodically that the agency is adhering to them. • Temporary or contract staff receiving less rigorous vetting than permanently employed colleagues carrying out similar roles.
Training and awareness	
• Providing good quality, standard training on anti-bribery and corruption for all staff. • Additional anti-bribery and corruption training for staff in higher risk positions. • Ensuring staff responsible for training others have adequate training themselves.	• Failing to provide training on anti-bribery and corruption, especially to staff in higher risk positions. • Training staff on legislative and regulatory requirements but failing to provide practical examples of how to comply with them. • Failing to ensure anti-bribery and corruption policies and procedures are easily accessible to staff.

Anti-bribery and corruption – consolidated examples of good and poor practice

Examples of good practice	Examples of poor practice
Training and awareness	
• Ensuring training covers practical examples of risk and how to comply with policies. • Testing staff understanding and using the results to assess individual training needs and the overall quality of the training. • Staff records setting out what training was completed and when. • Providing refresher training and ensuring it is kept up-to-date.	• Neglecting the need for appropriate staff training in the belief that robust payment controls are sufficient to combat anti-bribery and corruption.
Risks arising from remuneration structures	
• Assessing whether remuneration structures give rise to increased risk of bribery and corruption. • Determining individual bonus awards on the basis of several factors, including a good standard of compliance, not just the amount of income generated. • Deferral and clawback provisions for bonuses paid to staff in higher risk positions.	• Bonus structures for staff in higher risk positions which are directly linked (e.g. by a formula) solely to the amount of income or profit they produce, particularly when bonuses form a major part, or the majority, of total remuneration.

Anti-bribery and corruption – consolidated examples of good and poor practice	
Examples of good practice	**Examples of poor practice**
Incident reporting	
• Clear procedures for whistleblowing and reporting suspicions, and communicating these to staff. • Appointing a senior manager to oversee the whistleblowing process and act as a point of contact if an individual has concerns about their line management. • Respect for the confidentiality of workers who raise concerns. • Internal and external suspicious activity reporting procedures in line with the Joint Money Laundering Steering Group Guidance. • Keeping records or copies of internal suspicion reports which are not forwarded as SARs for future reference and possible trend analysis. • Financial crime training covers whistleblowing procedures and how to report suspicious activity.	• Failing to report suspicious activity relating to bribery and corruption. • No clear internal procedure for whistleblowing or reporting suspicions. • No alternative reporting routes for staff wishing to make a whistleblowing disclosure about their line management or senior managers. • A lack of training and awareness in relation to whistleblowing the reporting of suspicious activity.

Anti-bribery and corruption – consolidated examples of good and poor practice

Examples of good practice	Examples of poor practice
The role of compliance and internal audit	
• Compliance and internal audit staff receiving specialist training to achieve a very good knowledge of bribery and corruption risks. • Effective compliance monitoring and internal audit reviews which challenge not only whether processes to mitigate bribery and corruption have been followed but also the effectiveness of the processes themselves. • Independent checking of compliance's operational role in approving third party relationships and accounts, where relevant. • Routine compliance and/or internal audit checks of higher risk third party payments to ensure there is appropriate supporting documentation and adequate justification to pay.	• Failing to carry out compliance or internal audit work on anti-bribery and corruption. • Compliance, in effect, signing off their own work, by approving new third party accounts and carrying out compliance monitoring on the same accounts. • Compliance and internal audit not recognising or acting on the need for a risk-based approach.

The Financial Services Authority
25 The North Colonnade Canary Wharf London E14 5HS
Telephone: +44 (0)20 7066 1000 Fax: +44 (0)20 7066 1099
Website: http://www.fsa.gov.uk

Financial Services Authority