

## Chapter 9

# Anti-bribery and corruption in commercial insurance broking (2010)

## 9.1 Introduction

**9.1.1 Who should read this chapter?** This chapter is relevant, and its statements of good and poor practice apply, to:

- **commercial insurance brokers and other firms** who are subject to the financial crime rules in ■ SYSC 3.2.6R or ■ SYSC 6.1.1R; and
- **e-money institutions and payment institutions** within our supervisory scope.

Except that ■ FCTR 9.3.3G and ■ FCTR 9.3.4G only apply to those firms or institutions who use third parties to win business. It may also be of interest to other firms who are subject to ■ SYSC 3.2.6R and ■ SYSC 6.1.1R.

**9.1.2** In May 2010 the *FSA* published the findings of our review into the way commercial insurance broker firms in the UK addressed the risks of becoming involved in corrupt practices such as bribery. The *FSA* visited 17 broker firms. Although this report focused on commercial insurance brokers, the findings are relevant in other sectors.

**9.1.3** The report examined standards in managing the risk of illicit payments or inducements to, or on behalf of, third parties in order to obtain or retain business.

**9.1.4** The report found that many firms' approach towards high-risk business was not of an acceptable standard and that there was a risk that firms were not able to demonstrate that adequate procedures were in place to prevent bribery from occurring.

**9.1.5** The report identified a number of common concerns including weak governance and a poor understanding of bribery and corruption risks among senior managers as well as very little or no specific training and weak vetting of staff. The *FSA* found that there was a general failure to implement a risk-based approach to anti-bribery and corruption and very weak due diligence and monitoring of third-party relationships and payments.

**9.1.6** The contents of this report are reflected in ■ FCG 2 (Financial crime systems and controls) and ■ FCG 6 (Bribery and corruption).



## **9.2 The FSA's findings**

### **9.2.1**

You can read the findings of the *FSA's* thematic review here: [http://www.fsa.gov.uk/pubs/anti\\_bribery.pdf](http://www.fsa.gov.uk/pubs/anti_bribery.pdf)

## 9.3 Consolidated examples of good and poor practice

### 9.3.1

#### Governance and management information

Examples of good practice	Examples of poor practice
<ul style="list-style-type: none"> <li>• 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.</li> </ul>	<ul style="list-style-type: none"> <li>• Failing to allocate official responsibility for anti-bribery and corruption to a single senior manager or appropriately formed committee.</li> </ul>
<ul style="list-style-type: none"> <li>• 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.</li> </ul>	<ul style="list-style-type: none"> <li>• A lack of awareness and/or engagement in anti-bribery and corruption at senior management or Board level.</li> </ul>
<ul style="list-style-type: none"> <li>• Swift and effective senior management-led response to significant bribery and corruption events, which highlight potential areas for improvement in systems and controls.</li> </ul>	<ul style="list-style-type: none"> <li>• Little or no MI sent to the Board about higher risk third party relationships or payments.</li> </ul>
<ul style="list-style-type: none"> <li>• Regular MI to the Board and other relevant senior management forums.</li> </ul>	<ul style="list-style-type: none"> <li>• Failing to include details of wider issues, such as new legislation or regulatory developments in MI.</li> </ul>
<ul style="list-style-type: none"> <li>• 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.</li> </ul>	<ul style="list-style-type: none"> <li>• IT systems unable to produce the necessary MI.</li> </ul>
<ul style="list-style-type: none"> <li>• MI submitted to the Board ensures they are adequately informed of any external de-</li> </ul>	

developments relevant to bribery and corruption.

- Actions taken or proposed in response to issues highlighted by MI are minuted and acted on appropriately.

**9.3.2**

**Risk assessment and responses to significant bribery and corruption events**

Examples of good practice	Examples of poor practice
<ul style="list-style-type: none"> <li>• 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.</li> <li>• More robust due diligence on and monitoring of higher risk third-party relationships.</li> <li>• Thorough reviews and gap analyses of systems and controls against relevant external events, with strong senior management involvement or sponsorship.</li> <li>• Ensuring review teams have sufficient knowledge of relevant issues and supplementing this with external expertise where necessary.</li> <li>• Establishing clear plans to implement improvements arising from reviews, including updating policies, procedures and staff training.</li> <li>• Adequate and prompt reporting to SOCA (Serious Organised Crime Agency. See for common terms) and use of any inappropriate payments identified during business practice review.</li> </ul>	<ul style="list-style-type: none"> <li>• Failing to consider the bribery and corruption risks posed by third parties used to win business.</li> <li>• Failing to allocate formal responsibility for anti-bribery and corruption risk assessments.</li> <li>• Little or no MI sent to the Board about higher risk third party relationships or payments.</li> <li>• Failing to respond to external events which may draw attention to weaknesses in systems and controls.</li> <li>• Taking too long to implement changes to systems and controls after analysing external events.</li> <li>• Failure to bolster insufficient in-house knowledge or resource with external expertise.</li> <li>• Failure to report inappropriate payments to SOCA and a lack of openness in dealing with us concerning any material issues identified.</li> </ul>

**9.3.3**

**Due diligence on third-party relationships**

Examples of good practice	Examples of poor practice
---------------------------	---------------------------

<ul style="list-style-type: none"> <li>Establishing and documenting policies with a clear definition of a 'third party' and the due diligence required when establishing and reviewing third-party relationships.</li> </ul>	<ul style="list-style-type: none"> <li>Failing to carry out or document due diligence on third-party relationships.</li> </ul>
<ul style="list-style-type: none"> <li>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.</li> </ul>	<ul style="list-style-type: none"> <li>Relying heavily on the informal 'market view' of the integrity of third parties as due diligence.</li> </ul>
<ul style="list-style-type: none"> <li>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.</li> </ul>	<ul style="list-style-type: none"> <li>Relying on the fact that third-party relationships are longstanding when no due diligence has ever been carried out.</li> </ul>
<ul style="list-style-type: none"> <li>Taking reasonable steps to verify the information provided by third parties during the due diligence process.</li> </ul>	<ul style="list-style-type: none"> <li>Failing to respond to external events which may draw attention to weaknesses in systems and controls.</li> </ul>
<ul style="list-style-type: none"> <li>Using third party forms which ask relevant questions and clearly state which fields are mandatory.</li> </ul>	<ul style="list-style-type: none"> <li>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).</li> </ul>
<ul style="list-style-type: none"> <li>Having third party account opening forms reviewed and approved by compliance, risk or committees involving these areas.</li> </ul>	<ul style="list-style-type: none"> <li>Accepting vague explanations of the business case for using third parties.</li> </ul>
<ul style="list-style-type: none"> <li>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.</li> </ul>	<ul style="list-style-type: none"> <li>Approvers of third-party relationships working within the broking department or being too close to it to provide adequate challenge.</li> </ul>
<ul style="list-style-type: none"> <li>Routinely informing all parties involved in the insurance transaction about the involvement of third parties being paid commission.</li> </ul>	<ul style="list-style-type: none"> <li>Accepting instructions from third parties to pay commission to other individuals or entities which have not been subject to due diligence.</li> </ul>
<ul style="list-style-type: none"> <li>Ensuring current third-party due diligence standards are appropriate when business is acquired that is higher risk than existing business.</li> </ul>	<ul style="list-style-type: none"> <li>Assuming that third-party relationships acquired from other firms have been subject to adequate due diligence.</li> </ul>
<ul style="list-style-type: none"> <li>Considering the level of bribery and corruption risk</li> </ul>	<ul style="list-style-type: none"> <li>Paying high levels of commission to third parties</li> </ul>

<p>posed by a third party when agreeing the level of commission.</p> <ul style="list-style-type: none"> <li>• 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.</li> <li>• Paying commission to third parties on a one-off fee basis where their role is pure introduction.</li> <li>• 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.</li> <li>• Higher or extra levels of approval for high risk third-party relationships.</li> <li>• Regularly reviewing third-party relationships to identify the nature and risk profile of third-party relationships.</li> <li>• Maintaining accurate central records of approved third parties, the due diligence conducted on the relationship and evidence of periodic reviews.</li> </ul>	<p>used to obtain or retain higher risk business, especially if their only role is to introduce the business.</p> <ul style="list-style-type: none"> <li>• 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.</li> <li>• Leaving redundant third-party accounts 'live' on the accounting systems because third-party relationships have not been regularly reviewed.</li> <li>• Being unable to produce a list of approved third parties, associated due diligence and details of payments made to them.</li> </ul>
--	---

**9.3.4**

**Payment controls**

Examples of good practice	Examples of poor practice
<ul style="list-style-type: none"> <li>• Ensuring adequate due diligence and approval of third-party relationships before payments are made to the third party.</li> <li>• Risk-based approval procedures for payments and a clear understanding of why payments are made.</li> </ul>	<ul style="list-style-type: none"> <li>• Failing to check whether third parties to whom payments are due have been subject to appropriate due diligence and approval.</li> <li>• The inability to produce regular third-party payment schedules for review.</li> </ul>

<ul style="list-style-type: none"> <li>• Checking third-party payments individually prior to approval, to ensure consistency with the business case for that account.</li> <li>• Regular and thorough monitoring of third-party payments to check, for example, whether a payment is unusual in the context of previous similar payments.</li> <li>• A healthily sceptical approach to approving third-party payments.</li> <li>• Adequate due diligence on new suppliers being added to the Accounts Payable system.</li> <li>• Clear limits on staff expenditure, which are fully documented, communicated to staff and enforced.</li> <li>• Limiting third-party payments from Accounts Payable to reimbursements of genuine business-related costs or reasonable entertainment.</li> <li>• Ensuring the reasons for third-party payments via Accounts Payable are clearly documented and appropriately approved.</li> <li>• The facility to produce accurate MI to facilitate effective payment monitoring.</li> </ul>	<ul style="list-style-type: none"> <li>• Failing to check thoroughly the nature, reasonableness and appropriateness of gifts and hospitality.</li> <li>• No absolute limits on different types of expenditure, combined with inadequate scrutiny during the approvals process.</li> <li>• The giving or receipt of cash gifts.</li> </ul>
--	---

**9.3.5**

**Staff recruitment and vetting**

Examples of good practice	Examples of poor practice
<ul style="list-style-type: none"> <li>• Vetting staff on a risk-based approach, taking into account financial crime risk.</li> <li>• 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.</li> <li>• A risk-based approach to dealing with adverse in-</li> </ul>	<ul style="list-style-type: none"> <li>• Relying entirely on an individual’s market reputation or market gossip as the basis for recruiting staff.</li> <li>• Failing to check thoroughly the nature, reasonableness and appropriateness of gifts and hospitality.</li> <li>• Failing to consider on a continuing basis whether</li> </ul>



<p>formation raised by vetting checks, taking into account its seriousness and relevance in the context of the individual's role or proposed role.</p> <ul style="list-style-type: none"> <li>• 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.</li> <li>• Conducting periodic checks to ensure that agencies are complying with agreed vetting standards.</li> <li>• 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.</li> </ul>	<p>staff in higher risk positions are becoming vulnerable to committing fraud or being coerced by criminals.</p> <ul style="list-style-type: none"> <li>• Relying on contracts with employment agencies covering staff vetting standards without checking periodically that the agency is adhering to them.</li> <li>• Temporary or contract staff receiving less rigorous vetting than permanently employed colleagues carrying out similar roles.</li> </ul>
---	--

**9.3.6**

**Training and awareness**

Examples of good practice	Examples of poor practice
<ul style="list-style-type: none"> <li>• Providing good quality, standard training on anti-bribery and corruption for all staff.</li> <li>• Additional anti-bribery and corruption training for staff in higher risk positions.</li> <li>• Ensuring staff responsible for training others have adequate training themselves.</li> <li>• Ensuring training covers practical examples of risk and how to comply with policies.</li> <li>• Testing staff understanding and using the results to assess individual train-</li> </ul>	<ul style="list-style-type: none"> <li>• Failing to provide training on anti-bribery and corruption, especially to staff in higher risk positions.</li> <li>• Training staff on legislative and regulatory requirements but failing to provide practical examples of how to comply with them.</li> <li>• Failing to ensure anti-bribery and corruption policies and procedures are easily accessible to staff.</li> <li>• Neglecting the need for appropriate staff training in the belief that robust payment controls are sufficient to combat anti-bribery and corruption.</li> </ul>

- ing 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.

**9.3.7**

**Risk arising from remuneration structures**

Examples of good practice	Examples of poor practice
<ul style="list-style-type: none"> <li>• Assessing whether remuneration structures give rise to increased risk of bribery and corruption.</li> </ul>	<ul style="list-style-type: none"> <li>• 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.</li> </ul>
<ul style="list-style-type: none"> <li>• Determining individual bonus awards on the basis of several factors, including a good standard of compliance, not just the amount of income generated.</li> </ul>	
<ul style="list-style-type: none"> <li>• Deferral and clawback provisions for bonuses paid to staff in higher risk positions.</li> </ul>	

**9.3.8**

**Incident reporting**

Examples of good practice	Examples of poor practice
<ul style="list-style-type: none"> <li>• Clear procedures for whistleblowing and reporting suspicions, and communicating these to staff.</li> </ul>	<ul style="list-style-type: none"> <li>• Failing to report suspicious activity relating to bribery and corruption.</li> </ul>
<ul style="list-style-type: none"> <li>• 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.</li> </ul>	<ul style="list-style-type: none"> <li>• No clear internal procedure for whistleblowing or reporting suspicions.</li> </ul>
<ul style="list-style-type: none"> <li>• Respect for the confidentiality of workers who raise concerns.</li> </ul>	<ul style="list-style-type: none"> <li>• No alternative reporting routes for staff wishing to make a whistleblowing disclosure about their line management or senior managers.</li> </ul>
<ul style="list-style-type: none"> <li>• Internal and external suspicious activity reporting</li> </ul>	<ul style="list-style-type: none"> <li>• A lack of training and awareness in relation to</li> </ul>

<ul style="list-style-type: none"> <li>procedures in line with the Joint Money Laundering Steering Group guidance.</li> <li>Keeping records or copies of internal suspicion reports which are not forwarded as SARs for future reference and possible trend analysis.</li> <li>Financial crime training covers whistleblowing procedures and how to report suspicious activity.</li> </ul>	whistleblowing the reporting of suspicious activity.
--	--

**9.3.9**

The role of compliance and internal audit

Examples of good practice	Examples of poor practice
<ul style="list-style-type: none"> <li>Compliance and internal audit staff receiving specialist training to achieve a very good knowledge of bribery and corruption risks.</li> </ul>	<ul style="list-style-type: none"> <li>Failing to carry out compliance or internal audit work on anti-bribery and corruption.</li> </ul>
<ul style="list-style-type: none"> <li>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.</li> </ul>	<ul style="list-style-type: none"> <li>Compliance, in effect, signing off their own work, by approving new third party accounts and carrying out compliance monitoring on the same accounts.</li> </ul>
<ul style="list-style-type: none"> <li>Independent checking of compliance’s operational role in approving third party relationships and accounts, where relevant.</li> </ul>	<ul style="list-style-type: none"> <li>Compliance and internal audit not recognising or acting on the need for a risk-based approach.</li> </ul>
<ul style="list-style-type: none"> <li>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.</li> </ul>	

