

Compliance Monitor

The monthly briefing service for compliance specialists

Employee fraud – the internal storm

Employee fraud is rarely out of the news. Conferences, seminars and reports all assert that it is on the increase. However, writes Catherine Bunton of ebis risk services, despite the attention employee fraud attracts, it is still difficult to quantify and its true impact is rarely appreciated, except of course by those who have already fallen victim. It is hardly surprising when organisations are under increasing scrutiny from regulators, shareholders, investors and the public alike that they are reluctant to admit to its extent or very presence. Whilst it is an uncomfortable truth, it must be dealt with. Fortunately, there are measures that can be taken to alleviate the problem if the issue is addressed in a cogent way.

What is employee fraud?

Employee fraud might be defined as any action or actions perpetrated by an employee, or contractor or trusted third party causing, or having the potential to cause, financial harm to an organisation. However we define it, it is clear that the financial services sector suffers more than most. The FSA now appears to be adopting a more robust approach and has demonstrated through its recent actions that it is prepared to use both criminal prosecutions and financial penalties as it sees appropriate to deal with the problem.

Were the FSA's resolve in any doubt one needs only to consider the record breaking financial crime penalty it imposed on Aon Limited in January this year for the company's failings in its anti-bribery and corruption systems and controls. As a result of some US\$7 million of suspicious payments made to a number of overseas firms and individuals, the company was fined £5.25m and, had it not been for Aon's cooperation and the application of a 30% discount, that fine would have been an even more substantial £7.5 million.

The FSA gets tough

For those who may have considered the action against Aon a one-off, March saw the outcome of the first criminal prosecution brought by the regulator for insider dealing. The case concerned Christopher McQuoid, a solicitor and at the time an employee of TTP Communications, and his father-in-law, James Melbourne. The pair were each found guilty of insider trading following McQuoid divulging to Melbourne the fact that TTP were about to be acquired by the US

mobile giant Motorola, following which Melbourne acquired shares in TTP. Both McQuoid and Melbourne received custodial sentences of eight months, albeit Melbourne's case was suspended for 12 months. It is understood that the FSA are currently pursuing five other criminal prosecutions.

Identifying the problem

There can be little doubt that the problem is a serious one that organisations need to tackle not only from a regulatory perspective but also from the old-fashioned perspective of good business sense. But what should the regulated sector do and what should they be looking for?

Take a moment to think about the types of fraud your organisation may have already suffered, or the type of incident that is likely to manifest itself. The list of potential frauds is long, with insider trading, information theft, misrepresentation, infiltration and computer misuse high on the list. Whatever springs to mind these frauds all have one thing in common – the ability to have significant detrimental impact upon the organisation, whether in terms of operations, compliance, reputation, commercial viability or stakeholder confidence. It can leave the organisation open to civil and criminal proceedings and, of course, intervention by the FSA.

Were the previous examples not enough to strike fear into the hearts of all right-minded company officers and compliance professionals, May 2009 saw the FSA fine Morgan Stanley £1.4m for failing to prevent trader mis-marking. It also fined Matthew Sebastian Piper, a former proprietary trader at the firm, £105,000 and banned him from performing any regulated function. In another case the previous month the regulator, for the first time, banned and fined an individual for mis-marking trading positions.

For these reasons Compliance Officers need to be constantly alert to the warning signals heralding the presence of employee fraud, recognising the dangers that business processes and gaps and weaknesses within them present. They must also resist the temptation to dismiss as clichéd the well known warning signs that feature on every investigators list, such as employee lifestyle, reluctance to take leave, excessive working hours and high staff turnover.

The investigatory framework

If a suspected incident is identified, how should it be dealt with? The answer to this question is vital if the organisation gets it wrong then it may find itself not only suffering loss as a result of the fraud, but also as a result of being unable to effectively remedy the problem or, in some instances, with proceedings taken against it by the employee.

An incidence of employee fraud may be the first occasion that those charged with investigation will find themselves confronted with the requirements of three distinct but nevertheless overlapping regimes – criminal, civil and employment law. Firstly, therefore, we need to understand the requirements of those regimes to ensure that our processes meet the necessary standards and are compliant.

The rights of the employee must be considered from outset and there is much legislation to take into account. As a starting point, laws such as the *Employment Act 2008* and the statutory codes of practice will have considerable impact on how the investigation must be conducted and how the issues that may arise must be managed. Similarly, those charged with investigation should be familiar with the Civil Procedure Rules (CPR). It is important that the investigative team understand how these rules impact on planned actions. In addition, many fraud investigations in the financial services sector include elements of contract, copyright, interception of telecommunications and criminal law. Add a pinch of the *Human Rights Act 1998*, a sprinkling of *The Regulation of Investigatory Powers Act 2000* and a section or two of the *Fraud Act 2006* and it is clear that there is much to become acquainted with. However, we not only need to be aware of the relevant legislation, we must understand how it applies in practice to the investigative steps we intend to take.

So why do we need policies and procedures when there is such a complex external framework of laws and statutory regulation that already prescribe what must be done? Policies and procedures should not only take account of the working practices of the business and its corporate objectives, but should ensure that consistency and fairness are applied in all cases and that this can be demonstrated. We can probably all recount instances where individuals were dealt with differently from prescribed procedure and the can of worms that opens as a consequence. There have been many examples where an award has been made against the employer precisely because its own procedure was not followed.

Prevention versus cure

We all know that prevention is better than cure. An obvious statement but how many organisations apply

sufficient and proportionate resources to monitoring the enforcement of internal controls and creating a culture that frustrates and prevents fraud? How many compliance specialists can even say that they receive full inter-departmental cooperation in the event of a suspected incidence of fraud? In our experience this is worryingly uncommon.

It is a widely recognised concept that organisations will have disaster recovery and business continuity plans. These plans are designed to reduce panic, understand who should be doing what, facilitate the engagement of external resources and facilities, and speed business recovery. In the same way, the investigative readiness plan should document the relevant skill sets that are available internally and those that can be called upon from external experts as required. A cross-departmental team may include investigators, HR, internal audit and Compliance and, if the situation warrants it, public relations and direct Board level involvement. Once the plan is put into effect the investigation should be coordinated through one department that is prepared, and able to carry out, reporting responsibilities to the main Board.

It may be necessary or desirable to engage external experts to assist, but be aware that you are responsible for their conduct as part of the investigation, including unlawful or inappropriate behaviour – so choose wisely!

Once an incident occurs it is vital that time is not wasted. In our experience as much of 60% of time taken to deal with a fraud is spent in preparation due to a lack of planning and investigative readiness. It is also a requirement of the Advisory, Conciliation and Arbitration Service (ACAS) Code of Practice that investigations must be carried out without unreasonable delay. It may be wise to make this requirement known to those with permanently 'busy' diaries.

Creating an investigative plan

In all instances where a fraud is discovered an investigative plan specific to the incident should be created, which defines objectives and outlines proposed actions. The document must, of course, be dynamic in order to reflect changes in circumstances and evidence gathered as an investigation proceeds. Actions must also be documented, demonstrating compliance with legislation, regulation and company policy. It is considered wise to always work to criminal evidential standards to avoid problems with the quality of evidence or challenges to admissibility. A small matter that may be considered of little significance on first appearance, initially perhaps appearing to require only the reprimand of staff involved, may escalate to a matter that you wish

to put before police requiring a criminal prosecution. If the matter is not managed to a criminal standard at the outset it may be difficult to promote it accordingly.

The evidential trail

A significant part of any investigation will be to identify and secure relevant seats of evidence. Evidence may lie in a number of places both inside and outside the organisation. It may be in the form of verbal evidence of individuals, documentary or physical evidence, or indeed evidence maintained in IT systems. It is vital that evidence of whatever type is secured as soon as possible after it is identified because if left it may well start to degrade or indeed disappear altogether. This is particularly relevant to evidence that may be found in IT systems.

There will be very few frauds perpetrated today, particularly within the financial services industry and the regulatory framework within which it operates, that will not leave some form of forensic evidence on an electronic device, be it a computer system, phone, PDA, memory device, etc. More unusually, evidence may be uncovered on printers or even satellite navigation systems. The key, however, will be in establishing where the relevant information is likely to be found. If consulting external forensic experts, then it is wise to use their expertise to help to establish this and avoid loss of evidence and unnecessary expenditure. A reputable company will advise you on the most efficient means of uncovering relevant information and will be able to assist you in determining how any data discovered during forensic analysis fits within the overall investigation. However, it should be remembered that if you fail to brief a consultant fully on the investigation at hand you will not be using them to their full potential and will almost certainly miss evidence.

Forensic work must also be conducted to relevant evidential standards and it is vital that any external company engaged is aware of the legal environment

within which they are to operate, and are fully compliant with the relevant codes of practice.

It is highly unlikely that all of the relevant evidence will be confined to internal sources. As such, investigators should also look outside of the organisation for supporting evidence. Public records, media sources, and other resources that can be lawfully accessed, according to individual circumstances, such as web and chat group postings, can be invaluable in assisting with the tracing of assets and in discovering relevant associations and networks, but beware, just because information may be readily available does not necessarily mean that it can be lawfully accessed or used in the investigative process.

The way forward

Innovative fraud prevention techniques, coupled with a cogent investigative readiness plan, have the potential not only to achieve substantial cost savings, but also protect both reputation and stakeholder confidence. This is particularly relevant at a time when each of these commodities is in short supply and needs to be jealously protected.

Whilst it can be difficult to get the organisation behind a procedure that is formulated along these lines when there are so many other calls on resources, it must decide what it wants to achieve, both from preventative measures and from each individual investigation. It is a question of deciding what is appropriate and effective. There is, of course, the 'do nothing' option, but beware; these matters rarely, if ever, remedy themselves.

By adopting a dynamic approach the cloud of employee fraud can at least have a silver lining, rather than turning into a particularly unpleasant and costly storm.

© 2009 ebis risk services ltd. *Catherine Bunton* is a director of ebis risk services, a specialist risk management and investigations consultancy. For further information visit www.ebis.co.uk or telephone +44 (0)20 7531 9555.

Editor: Timon Molloy • Tel: 020 7017 4214 • Fax: 020 7436 8387 • Email: timon.molloy@informa.com

Editorial board: Mazhar Manzoor – Principal consultant, FSA Compliance Consultants Ltd • Denis O'Connor – Senior Compliance Executive, Commerzbank • Emma Radmore – Senior Solicitor, Financial Markets & Regulation Practice, Denton Wilde Sapte • Philip Ryley – Head of Financial Services and Markets, Michelmores LLP • Adam Samuel – Independent Compliance Consultant, Adam Samuel Training & Consulting Services • Richard Warrington – Head of Regulatory Affairs and Compliance, National Australia Group

Production Editor: Frida Fischer • Tel: 020 7017 5501 • Email: frida.fischer@informa.com

Publisher: Victoria Ophield

Sales and renewals: Pauline Seymour • Tel: +44 (0) 20 7017 5063 • Email: pauline.seymour@informa.com

Subscription orders and back issues: Please contact us on 020 7017 5532 or fax 020 7017 4781.

For further information on other finance titles produced by Informa Law, please phone 020 7017 5063

Printed by Premier Print Group • This newsletter is printed on paper from sustainable forests.

ISSN 0953-9239 © Informa UK Ltd

Published 10 times a year by Informa Law, Telephone House, 69-77 Paul Street, London EC2A 4LQ. Tel 020 7017 5000. Fax 020 7017 4601. www.informa.com

Copyright: While we want you to make the best use of Compliance Monitor, we also need to protect our copyright. We would remind you that copying is illegal.

However, please contact us directly should you have any special requirements.

While all reasonable care has been taken in the preparation of this publication, no liability is accepted by the publishers nor by any of the authors of the contents of the publication, for any loss or damage caused to any person relying on any statement or omission in the publication. All rights reserved; no part of this publication may be reproduced, stored in a retrieval system or transmitted in any form or by any means, electrical, mechanical, photocopying, recording, or otherwise without the prior written permission of the publisher.

Informa UK Ltd, Registered Office: Mortimer House, 37/41 Mortimer Street, London, W1T 3JH.

Registered in England and Wales No 1072954.

informa
law
an informa business