

Fraud Intelligence

For the prevention, detection and control of fraud in all its guises

Building bridges

The Mabey & Johnson guilty plea to charges of overseas corruption and breaching sanctions in Iraq, which cost it UK£6m in fines and compensation on 25 September, is a “landmark outcome” as Richard Alderman, Director of the Serious Fraud Office (SFO), claimed. A question remains though over his observation that the conviction was “satisfyingly, achieved quickly.” After all, the firm was named in the Independent Inquiry Committee report on the UN Oil for Food Programme back in October 2005. But, by the grindingly slow standards of fraud litigation, perhaps he’s right.

Southwark Crown Court heard that the specialist bridge manufacturer self-reported to the SFO that it had paid off public officials in Jamaica and Ghana between 1 January 1993 and 31 January 2001. Further investigation revealed bribes offered in Madagascar, Angola, Mozambique and Bangladesh and a reference in a memo to use of “the white man’s handshake” to build trust and confidence before contracts were signed. The firm finally pled guilty to two counts of conspiracy to corrupt in Ghana and Jamaica and to “making funds available” in Iraq between 1 May 2001 and 1 November 2002.

Mabey & Johnson may be keen to draw a line under the matters but various of its employees still face possible criminal charges. They might argue that their chances of a fair hearing have been prejudiced by the firm’s admission.

The SFO meanwhile will be hoping that the decision persuades other companies to step up and confess but is this likely? The threat of disbarment from tenders for public contracts would argue not. On the other hand, directors may well be twitchy at the *Proceeds of Crime Act 2002* implications if bribery is brought to their notice. Mere possession of criminal property – which would cover any revenue and, by extension, directors’ remuneration secured through kickbacks, or even facilitation payments – counts as laundering and is punishable by up to 14 years in jail. If the board believes it is able to prevent bribery becoming public it may yet sit tight to avoid drawing fire, not only from the SFO but from overseas, notably, US criminal authorities; then there is also the unpleasant prospect of suits from angry shareholders should the share price fall once the news breaks.

One point at least is clear: the whole issue is not about to go away. BAE, the defence contractor, investigated over alleged bribes to secure the al Yamamah arms deal, until the Government intervened, is now looking at another SFO prosecution for possible illegal payments in connection with aircraft sales in South Africa and the Czech Republic, frigates to Romania and radar equipment for air traffic control in Tanzania. “If... proceedings are commenced,” said BAE, “the company will deal with any issues raised in those proceedings at the appropriate time and, if necessary, in court.”

Timon Molloy, Editor

October/November 2009

IN THIS ISSUE

- 1 Building bridges**
First UK guilty plea for overseas corruption but how many more?
- 2 News**
- 3 Out of court**
The European Court of Auditors chief has a little (wish)list
- 5 Overseas corruption guidance: another step to deferred prosecution agreements?**
- 7 Surgical strike**
Latest technology accelerates document searches
- 9 The stable door is still open!**
Case studies in alternative fraud risk management
- 12 Ethics in a Web 2.0 world**
Facebook to Twitter – social media exposure
- 14 See the future – and prevent it**
A forensic accounting approach to fraud control

**Financial Crime Congress
Online**

‘Shah v HSBC’
with Nicholas Medcroft
of Outer Temple Chambers
27 October 2009 at 16:00 BST
Global, via the Internet
www.i-lawcongress.com

informa
law

down the pecking order whenever an investigation is on (which is most of the time in many large and medium sized organizations). Following on the rules of thumb given above there are some simple guidelines, which we believe can make life easier and break the continuous cycle of investigations. The key is to learn to Predict, Pre-empt and Prevent fraud and corruption. There are some straightforward ways to do this:

- management and staff should participate in simple ‘think like a thief’ exercises in order to start looking at the company from a fraudster’s perspective. This is the basis of profiling by which the company identifies its major fraud exposures;
- techniques should be developed to detect red flags early. [5] This might lead to a number of ‘micro’ investigations but these are very easy to manage;
- discretion is a cornerstone of any investigation steps should also be taken before, during and afterwards to make people more aware of the threats of fraud, corruption and unethical business behaviour. Prepared and alert employees are an invaluable resource in helping make companies resistant and resilient. Sending a message across the organisation (by de-heading the snake, as discussed in the second case study) may be just what is needed.

Several years ago, senior management in one organisation informed said, “We want to give you our full support for the excellent work you are doing with internal controls to prevent fraud, and also the investigations you have carried out. However we are not so sure about this proposal of yours to detect lots of fraud. I mean what are we going to do with all the frauds you find... investigate them all?”

Thankfully, our clients today are much more proactive, support the use of fraud detection techniques and accept the temporary increase in the number of fraud investigations but not necessarily the size of them. We believe it is the way of the future.

Notes

1. “A new approach for a new era” by Jim Gee, *Fraud Intelligence* August/September 2009
2. “All just one big lie” by Timon Molloy, *Fraud Intelligence* February/March 2009
3. See note 1 above.
4. “Revising a Definition of Corruption as a Result of the Global Economic Crisis - The Case of Iceland, in *Organizational Immunity to Corruption: Building Theoretical and Research Foundations*,” Vaiman, V., Davidsson, P.A., & Sigurjonsson, T.O., Warsaw: Polish Academy of Sciences.
5. “Pre-emptive strike” by Richard Minogue and Nigel Iyer, *Fraud Intelligence* April/ May 2009

Nigel Iyer (nigel.iyer@septiagroup.com) originally trained as a Chartered Accountant but has worked in the prevention, detection and investigation of fraud and corruption for over 20 years. He is the author of “*Fraud and Corruption Prevention and Detection*” and the management novel “*The Tightrope*”. Today he writes drama and screenplays about the human effects of corruption and holds a Masters Degree in Screenwriting. His latest book, “*A Short Guide to Fraud Risk*” for CIMA and published by Gower, will be out in early 2010. Only one chapter out of seven is about investigations.

Veronica Morino (veronica.morino@septiagroup.com) has over the past ten years applied her academic training in sociology and science of the organisation to the field of fraud and corruption, first investigating many frauds and then focusing on prevention; she is working on measuring the resistance and resilience of organisations to fraud and corruption. Her book, “*The Anatomy of Fraud and Corruption*” (Morino, Minogue and Brytting) will be published in 2010.

Ethics in a Web 2.0 world

Exponential growth in social media presents the double edge of all technical innovation, a force for good but also expanded potential for the devious. Ethics policies must keep pace, says Luis Ramos, CEO of The Network.

More than 250 million users spend more than five billion minutes each day, worldwide, on Facebook. [1] In January of this year, 735,000 unique visitors accessed Twitter through their mobile phones. [2] Social network and blogging sites are now the fourth most popular activity on the internet, and time spent

on these sites is growing at over three times the rate of overall internet growth. [3]

As organisations increasingly witness the explosive growth of social media, they are recognising that what was once considered a fad is now a force too powerful to ignore, with vast new possibilities for creating, collaborating and communicating. Anyone who is not already blogging, bookmarking, tweeting, posting or chatting, is wondering if they should be.

Creating a social media strategy is a complex exercise, because it includes not only looking *inside*

the organisation to establish appropriate practices, policies and parameters for employees but also looking *outside* the organisation to determine what makes sense in terms of its own degree of engagement. Organisations want to leverage the rich opportunities afforded by emerging technologies, but they are also concerned about mitigating the risks associated with putting themselves, their brand and their reputation “out there”.

What is your policy?

Most organisations have a code of conduct that defines what is appropriate – and what is not – when it comes to acting with integrity on the job. Today, factoring the use of social media into the total equation of business conduct is fast becoming a critical best practice.

Some organisations with well-crafted policies about topics such as acceptable communication, protection of proprietary information and safeguarding corporate assets simply extend an employee’s responsibility for doing the honest, ethical thing into cyberspace. But other organisations find that a specific set of guidelines built around specific media sites (eg, “Don’t post any information about our company on Facebook.”) trump policy that is more broad (“Don’t compromise the integrity of our company.”)

The best approach is often a customised approach, one that will both mitigate its organisational risk and mesh with its organisational climate. In drafting guidelines that “fit,” policymakers tend to engage their legal team and corporate communications department to ensure legal bases are covered and tone/voice are consistent with their corporate brand.

A written social media policy offers a great venue for reminding employees that they are personally responsible for the content they publish online and that their posts are neither private nor sacred. In general, employees need to understand that anything that is not okay in the workplace is not okay online, and that speaking ill of their job, their boss or their co-workers can lead to serious consequences.

Organisations around the world are weighing in on similar social media policy issues, so it’s a fortuitous time to canvass what others are doing. For example, social media policies from more than 80 companies can be found at <http://socialmediagovernance.com/policies.php>. Policy penned (and published online) by Intel, IBM and Sun Microsystems is also widely referenced by organisations as they take on the process of crafting their own guidelines.

Moving from policy to possibilities...

Taking a look inside and developing policy around employee use of social media is a valuable exercise, but adopting strictly a defensive strategy can shortchange an organisation. The Web 2.0 world offers an excellent opportunity to harness technology to engage employees, explore the ethics landscape and shape the perception of ethics and compliance departments as resources, not watchdogs.

Organisations with a dedicated ethics and compliance page on their corporate intranet, for example, may find that the addition of a blog or discussion forum can prove to be a valuable tool for furthering the dialogue about ethics. Given the recent spate of unethical business practices in the news, there should be no shortage of conversation starters. A blog allows employees to voice their opinions, ask questions about their company’s policy and problem-solve based on their company’s code. Organisations can also use the forum for providing policy updates and links to reputable sources of information.

If contemplating a discussion forum, organisations are wise to include a notice up front that the blog is not the right place for reporting misconduct or disclosing personal information. The Ethics Office doesn’t want to find out about a conflict of interest or other indiscretion in this forum. Instead, the blog can point employees to the proper resources for reporting job-specific issues or code of conduct violations.

It’s also a good idea to evaluate availability of resources to properly manage and monitor the site up front. A slow response – or no response – can effectively shut the dialogue down. And an inflammatory or objectionable post should be seen and dealt with immediately, keeping in mind, however, that the ability for readers to leave comments in an interactive format is an important part of the blog. Someone from the organisation should moderate, of course, but comments about tough topics can create a viral effect and ramp up the quantity and quality of posts.

Leveraging other social media to promote an ethical culture

Developing an Ethics and Compliance Facebook page can give organisations another means for talking with – instead of at – employees about ethical issues. As a best practice, organisations tend to assign a specific individual to create and manage the page and make sure they respond to messages and questions left on the organisation’s discussion board and wall within 24 hours.

A Facebook page is also a great forum for posting training event information or videos or using the site's group feature to network with an organisation's target audience or other industry groups. Want to gauge employee reaction to a recent corporate gaffe making the headlines? Facebook can be used to conduct polls and market research. Organisations should be aware, however, that data will be qualitative in nature, not quantitative, as it will represent the views of a portion of its workforce.

Twitter, too, offers an interactive forum for the exchange of ideas. Organisations can distribute short messages that direct readers, via URL, to ethics-relevant websites, blogs or intranet sites or insightful tone-from-the-top posts from company management. Of course, simply building a Facebook page or Twitter account will not invite readership and sharing. It is critical that an organisation's social media platform offers something of value and that a particular strategy is developed for attracting – and maintaining – fans. If an organisation uses the tool to deliver policy directives and behavioural expectations or a laundry list of events and e-mails it has already sent to employees (ie, reverting to talking *at* employees, instead of *with* them), the organisation can miss a wonderful opportunity to move ethical decision-making from policy to practice.

If full-scale immersion into the world of social

media feels too ambitious, organisations can explore other, less-public-facing tactics for promoting an ethical workplace. For example, they might monitor the conversation around ethics by following what ethical leaders are saying or participating in industry blogs and newsgroups or setting up a Google or Yahoo! alert to automatically receive e-mail updates regarding a particular query or code topic.

The fact is, whether an organisation is in a position to seize or simply size up the opportunities offered by social media, it is in good company, as organisations around the world begin to navigate the Web 2.0 waters.

Notes

1. Facebook Press Room, www.facebook.com/press/info.php?statistics, as of 11 September 2009
2. 'Twitter's Tweet Smell of Success', <http://blog.nielson.com/nielsenwire>, 18 March 2009
3. 'Global Faces and Networked Places', A Nielson Report on Social Networking's New Global Footprint, March 2009, pp 2-3.

Luis Ramos may be contacted at LuisRamos@twinc.com. The Network, Inc (www.twinc.com) provides customised reporting for documenting concerns, claims and incidents; service features include high quality assurance, rapid dissemination of data to key stakeholders, centralised, secure case management, advanced reporting analytics and comprehensive communications to engage employees.

See the future – and prevent it

*Great detectives collect fingerprints, examine evidence, and conduct interviews to figure out what happened at a murder scene. Likewise, it is a forensic accountant's job to detect fraud based on the evidence. But what, asks **Ivan A. Garces**, if the detective - or the forensic expert - could see the future, and keep the victim safe from harm? Wouldn't that be better?*

According to the Association of Certified Fraud Examiners (ACFE), "nearly half of the [fraud] cases in our 2008 study were uncovered by a tip or complaint from an employee, customer, vendor, or other source." [1] While the percentage discovered due to internal controls has increased since their 2006 report (now it's just over 23%), these programmes are still far from eliminating fraud, particularly in smaller businesses. In fact, 20% of the frauds studied were only discovered by accident.

A smart business owner can protect his business and assets by using a forensic accounting expert to perform a thorough risk assessment: to assess the risks of fraud,

quantify them, and put controls in place to help mitigate them.

Assess the environment for risk

The first step in performing a risk assessment is similar to the first move in a forensic investigation: *assess the level of risk by looking at the environment.*

What ethical environment has management created? What kind of example is the boss setting? Has it been clearly communicated that this company is an organisation with strong integrity? This concept applies in every type and size of business. The owner of a small company might run his personal expenses through the business; the CEO of a larger company could use questionable accounting procedures to make financial results appear more favourable. Excessive pressure from management to meet goals at any cost shows a tolerance for fraud.

Conduct interviews at every level. Talk to people in the executive suite, board members, middle management,