



FORENSIC

Fighting Fraud

Issue 29 Summer 2010

ADVISORY



Editorial

Ken Milliken

Welcome to the latest issue of *Fighting Fraud*. Since the last edition we have seen several major frauds reported in the press, contributing to a peak of £1.3 billion worth of cases in 2009 in the UK alone according to our research which only measures cases above £100,000 that come to court. The 2000s were a decade of fraud – the ‘naughty noughties’¹.

A Snapshot

DOJ cracks \$9m fraud ring²
The US Department of Justice (DOJ) has indicted an Eastern European crime ring for stealing £5.37m in a bank hacking operation. The gang hacked into a bank’s payroll system to clone cards and withdrew \$9m from 2,100 ATM machines in 280 cities, in just 12 hours. The DOJ have described it as “perhaps the most sophisticated and organised computer fraud attack conducted”.

Watchdog fines bank £8m for banking fraud³.

The FSA fined a bank for failing to prevent employees carrying out

unauthorised transactions with customer money – this is the third highest penalty the FSA has ever imposed. In addition to the fine, the bank also had to pay out £29.5m in compensation to clients whose accounts had been tampered with.

Telecommunication deal in Ghana attracts SFO interest⁴.

UK prosecutors are looking into allegations of possible fraud over the purchase of a 70 percent stake in the telecommunications company. According to an investigation of the deal commissioned by Ghana’s government Ghana didn’t get value from the sale because of a series of complicated financial arrangements.

This large total value of UK fraud shows a contrasting picture; on one hand companies are clearly becoming better attuned to the signs of fraud. With greater focus on corporate governance and the introduction of new laws and regulations to combat fraud, criminals are being identified and prosecuted

at a greater rate. On the other hand; despite the great efforts made to tackle white collar crime, criminals are continuously evolving the methods they use to commit fraud and conceal their actions. Organisations will need to remain vigilant as the problem of fraud is unlikely to ever be totally eradicated.

As we embark on a new decade, this edition looks forward at the preventative measures and proactive opportunities available to organisations to reduce the impact when a fraud is discovered.

In the first of our articles we look at insuring against the risk of fraud. If a fraud is conducted internally by a trusted employee, an insurance policy can significantly reduce the impact on a company’s bottom line. A policy of this type adapted to relevant jurisdictions can be an essential component of fraud prevention arrangements. This is especially relevant now, as companies are taking their activities to new, perhaps higher-risk, territories to survive the efforts of the global recession.

1 KPMG’s Fraud Barometer, January 2010
2 www.v3.co.uk/v3/news/2252912/feds-break-9mil-fraud-ring
3 www.fsa.gov.uk/pages/Library/Communication/PR/2009/150.shtml
4 www.ft.com/cms/s/0/d8459758-c817-11d1-8ba8-00144feab49a.html




Our second article looks at the greater challenges multinationals face to protect both their capital and reputation when setting up activities in these high growth markets. Fraud remains a worldwide problem and one that has no boundaries. Every organisation should give itself a head start against fraud by tailoring systems and controls to the cultures of the countries in which it operates to effectively prevent, detect and respond to fraud and misconduct.

As crime and criminals have become increasingly sophisticated, so too have their efforts to conceal money and assets worldwide, often beyond the reach of law enforcement. The third article in this edition looks at the work of forensic accountants who navigate through the web of misdirection to track down and recover the proceeds of a criminal act.

As the economic recovery progresses and businesses continue to look for new opportunities for growth, our

fourth article focuses on the Nigerian banking sector and the recent changes that have been put in place both to foster a more ethical business culture and to encourage new entrants to what is often perceived as a region with inherent bribery and corruption.

This edition rounds off by addressing the use of technology. Technology has for many years been an important tool in investigations. Our last article takes a specific look at the legal barriers in Germany when using e-disclosure techniques in fraud investigations.

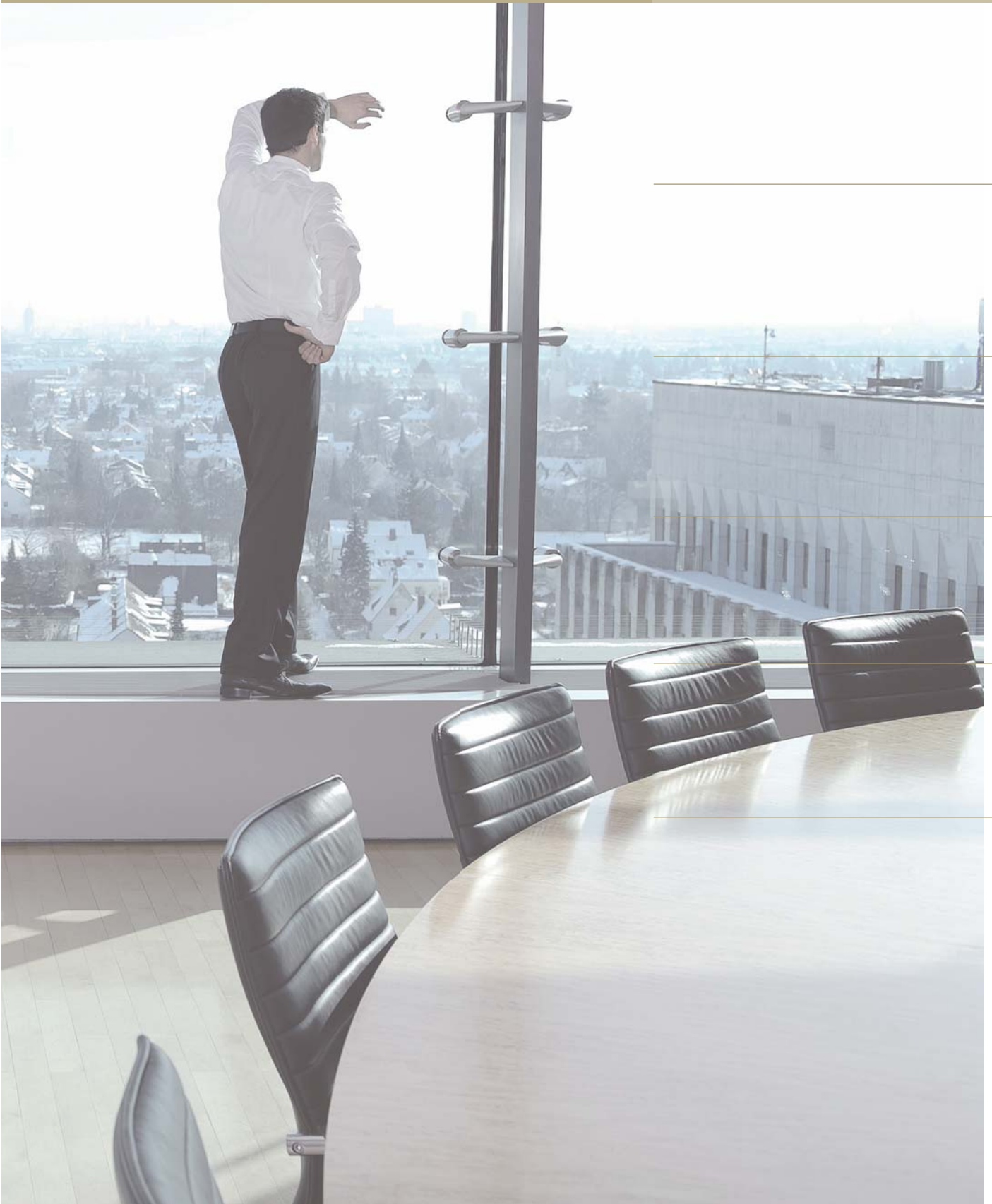
I hope you enjoy this edition and would be happy to answer any queries which are prompted by these articles. 



Ken Milliken

Associate Partner
KPMG Forensic practice in the UK
+44 (0) 141 300 5857
ken.milliken@kpmg.co.uk

Contents



06



Insuring Against the Risk of Fraud – Is it Worth it?

David Hicks | Georg Lochner | David Fidan

10



Fighting Fraud and Corruption in High Growth Markets

Alex Plavsic | Ken Milliken | Brent McDaniel

14



The Role of Corporate Intelligence in Tackling Organised Criminality

Roger Aldridge | Tom Russell | Tracey Wright

16



Fighting Fraud in Nigeria – What Progress has been Made?

Steven Haynes

18



e-Disclosure in Germany – Legal Barriers and Technological Potential

Helmut Brechtken | Tom Hopkinson | Thomas Fritzsche

22



Cases in Point

A selection of case studies from across a range of sectors and territories

The current economic situation is not only affecting the level of business activity, it is also proving to be a key driver of fraud on businesses, both internal and external. Losses due to fraud directly impact bottom line profits. Given the experience of increased frauds in the previous recession of the early 1990s, and the severity of the current conditions, firms should consider what can be done to reduce this impact. David Hicks, Partner, KPMG Forensic practice in the UK, Georg Lochner, Director, KPMG in Germany and David Fidan, Partner, KPMG in Switzerland, consider the use of fraud insurance as part of the strategy.

Insuring Against the Risk of Fraud – Is it Worth it?

David Hicks

Georg Lochner

David Fidan



“A long standing employee is not an indicator of reduced fraud risk.”

Introduction

There are a range of measures that firms can take not just to prevent and detect potential fraud, but also in planning their response to fraud should it occur. Measures include basic internal controls, such as segregation of duties and authorisation procedures, implementing whistle blowing procedures, through to reporting matters to the police, and initiating recovery of funds. Another action that firms can take is to ensure that they have appropriate insurance coverage should they become a victim of fraud.

The purpose of fraud insurance cover (commonly called Fidelity Insurance or Employee Dishonesty Insurance) is to insure companies against the financial losses from fraud committed by their own employees. In the event that a company suffers an internal fraud, the policy may compensate the organisation for the extent of the financial losses suffered and investigation costs.

Fraud Factors and Typologies

Whilst firms may be able to get insurance cover should they fall victim to fraud, there are a number of considerations. These include: cost, thresholds, time period and relevance. With regard to the last point, consideration should be given to whether the cover is for directors, management and/or staff, or whether it is to cover all types of personnel.

Fraud insurance most commonly covers employee frauds rather than frauds perpetrated by outsiders. As a result, most policies may not cover an investor in, for example, the Madoff funds for losses suffered as a result of the fraud, unless in the unlikely event that an employee could be proven to be complicit. The frauds which companies most commonly seek cover for are:

- 1) False (“ghost”) employees set up on payroll with salary payments then made out to them
- 2) Non-existent suppliers set up with payments made to them
- 3) Cheque fraud
- 4) Creation of false invoices
- 5) Theft of sensitive company or customer data
- 6) Embezzlement of physical company assets or property
- 7) Theft of petty cash

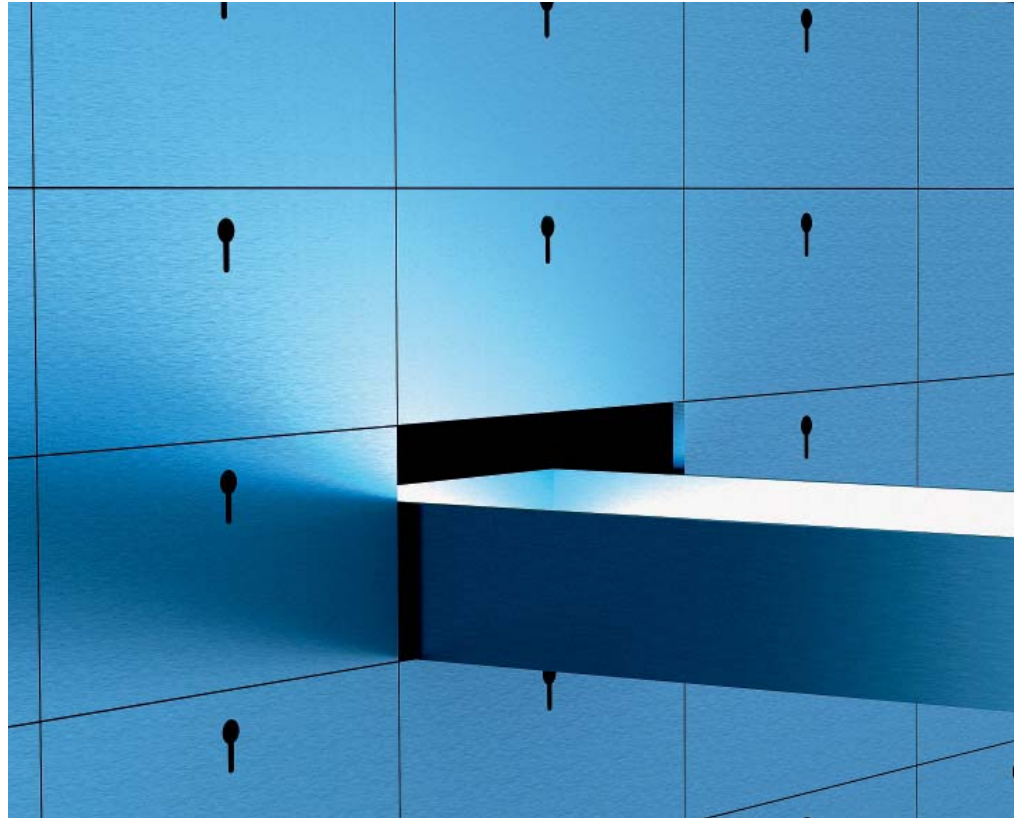
Issues

Organisations have provided several reasons that have prevented them taking adequate fraud insurance. The four main reasons were:

- 1) Trust placed on employees
- 2) Reliance on Controls
- 3) Cost/benefit of fraud insurance
- 4) Product issues

8 Fighting Fraud

Insuring Against the Risk of Fraud – Is it Worth it?



a) The Trusted Employee

Despite many high profile employee frauds over the years, companies quite rightly continue to place significant trust in their workforce. Companies usually put controls in place over key processes, but in our experience clever employees, particularly management, are usually able to find ways of bypassing controls.

In the worsening economic environment, the number of employee frauds is expected to rise. Contrary to expectations, a long standing employee is not an indicator of reduced fraud risk; in fact, quite the contrary. KPMG's own statistics from fraud cases that have come to court suggests that almost a third of fraudsters have been employed by their company for between 10 and 25 years.

b) Reliance on Controls

The controls companies have within their businesses may provide to senior directors a sense of security around the risk of fraud. Often large control implementation projects, requiring a substantial IT spend, serve to provide this comfort and, when coupled with internal and external audits, may serve to reassure the board that the risk of fraud is low.

This reliance is often misplaced however. Even the most common controls, such as electronic passwords, are routinely broken in circumstances where for example small teams have individuals on holiday or off-sick; without sharing of passwords, an employee may argue, the business could not function during such periods. Equally, recent high profile frauds have occurred at companies which are extensively audited and have mature control environments.

c) Cost/Benefit of Fraud Insurance

Research indicates that companies remain unconvinced by the cost/benefit analysis of fraud insurance. A scenario in which a fraud insurance policy pays out is one in which a company's controls have failed; many companies would rather trust in their employees and the robustness of their controls rather than incur the costs of fraud insurance.

d) Product Issues

One of the main drivers preventing higher uptakes of fraud insurance seems to be the typical policy wordings which are used. The two main issues here seem to be:

Exclusions: many policies are written with the condition that certain controls are in place and are operating

effectively, such as electronic passwords and building security. Where this is shown not to be the case, insurers are likely to decline a claim.

Completeness of Cover: there appears to be some confusion in the marketplace around exactly what risks are covered by fraud insurance. In addition to 'traditional fraud' risks, Marsh, the insurance broker, has noted an increase in companies requiring computer and data-related fraud insurance within recent years. With the intense focus on data security in both public and private organisations, providers of fraud insurance have had to adapt their policies to address these emerging risks, yet companies remain unclear on what protection fraud insurance provides.

The Recession – What Impact Will it Have?

The last twelve months have seen an increase in a range of frauds with 2009 peaking at £1.3bn¹. The recession is clearly adding increased pressure to all concerned, reduced levels of pay and rising costs as well as the increasing threat of redundancies. Those committing fraud have become more sophisticated in their efforts to

¹ KPMG's Fraud Barometer, January 2010



Although specific numbers for the sub-line fidelity insurance are not available, the latest figures published by the Germany Insurance Association show total premium income equal to €1.4bn for credit insurance, surety insurance and fidelity insurance in 2007.

Occasionally, fidelity insurance is, erroneously, considered a general type of D&O insurance (Directors' and Officers' liability insurance). This is certainly a misunderstanding. While any misdeeds of directors and officers are covered by a fidelity insurance, a D&O insurance first and foremost protects the firm's directors and senior executives against litigations actions and indemnification payments in connection with poor management decisions and other such acts committed in good faith. Criminal offenses (i.e., acts committed in bad faith) are not covered under a D&O insurance which generally contains exclusions for any losses incurred as a result of a deliberate act or knowingly violation of duties of directors and officers.

manipulate systems and controls to release money and in the concealment of their actions. Another contributing factor is the squeezing of management and administration costs, opening up new gaps in processes and hence new opportunities for fraud. Whilst Professional Criminals remain the most adept of fraudsters, pocketing over £700million in 2009, employee and management frauds combined cost UK businesses upwards of £565million. Since 2007 the number of cases directly involving Insurance companies has increased threefold, a statistic made more worrying by the fact that these cases were committed by a diverse range of perpetrators.


European Perspective

Within Germany the number of insurance companies offering fidelity insurance is limited. Typically, these are special insurers engaged in credit or surety insurance. A major player in Germany and Europe is Euler + Hermes which forms part of Allianz group. Other providers of fidelity insurance in Germany are HDI-Gerling (part of Talanx group) or R+V (part of the cooperative finance network). On an international level, AIG, CHUBB or ACE are engaged in this type of insurance business. Clearly the major providers in Germany are common to the UK as they are for other EU countries.

A Case of History Repeating

To those with long memories, we have been here before. At the height of the last recession, in August 1992, the Independent ran an article entitled "Ignoring the threat from within". The article highlighted the low sales of fidelity insurance at a time when employee fraud was growing at an alarming rate and contained following prescient words: "the Association of British Insurers says 'all types of claims involving dishonesty are on the up and up'. General Accident estimates one in three firms have been the victim of a fraud costing at least £50,000 in the past three years. But only one in seven thinks it worth insuring against." This contradictory statistic remains true today, with uptake of fraud insurance still much lower than actual instances of fraud.

Conclusion

When thinking about whether to take fraud insurance, the reasons not to take cover, as listed in this article, do not always stack up. For financial peace of mind and good governance companies should evaluate their fraud exposure and the benefits fraud insurance can provide. However, in a market of tightening budgets, the evidence shows that companies remain willing to run the risk of fraud rather than ensure they are protected against it. 



David Hicks

Partner
KPMG Forensic practice in the UK
+44 (0) 20 7694 2915
david.hicks@kpmg.co.uk



Georg Lochner

Director
KPMG Forensic practice in Germany
+49 89 9282 1610
glochner@kpmg.com



David Fidan

Partner
KPMG in Switzerland
+41 44 249 47 14
davidfidan@kpmg.com



Fighting Fraud and Corruption in High Growth Markets

Alex Plavsic
Ken Milliken
Brent McDaniel



Introduction

There has been an explosion of media headlines reporting investigations, prosecutions, and settlements of bribery and corruption violations involving major multinational companies and their executives, directors, and employees, often in emerging high growth markets. It is evident that preventing, detecting, and responding to international fraud and corruption is an increasingly difficult challenge.

Alex Plavsic and Ken Milliken from KPMG Forensic practice in the UK explore the challenge of preventing, detecting and responding to international cross-border fraud, corruption and misconduct in dynamic high growth markets.

In our experience, multinationals that invest in high growth markets for the first time frequently underestimate the risks inherent in many of these markets. It is not merely the different cultural traditions and attitudes towards acceptable business practice which exist in many economies which leads to increased risk. There are also issues arising from different legal systems, the high levels of autonomy often given to start ups in new territories, reliance on agents and reliance, at least initially, on a small group of potential customers or a joint venture partner.

All of this can add to pressures which can lead to fraud, bribery and corruption. Cases we have investigated include employees taking advantage of remoteness and a lack of oversight to boost personal earnings through procurement fraud, employees paying bribes to win that first large contract which cements the future of operations in that region and employees mis-reporting results in order to meet growth expectations and to secure new investment.

Prevention

KPMG's Overseas Bribery and Corruption Survey 2009 questioned 109 individuals responsible for compliance with anti-bribery and corruption legislation within FTSE Allshare companies. They were asked about their knowledge of both the US and UK regulatory framework as well as what steps their organisation is taking to ensure compliance with these regulations. The survey found that two thirds of respondents believe there are places in the world where they cannot do business without

engaging in bribery and corruption. However, despite this, over half of the respondents have not taken the decision to opt out of doing business there. Therefore the risks have to be addressed

In respect of bribery and corruption, not all high growth markets are the same. However, most high growth markets, including the BRIC economies, sit well below the UK and Western European countries when considering Transparency International's 2009 Global Corruption Perceptions Index, the annual index ranking countries according to the perceived level of corruption among public officials.

The fundamental issue to be borne in mind is that the fraud, bribery and corruption risks associated with operating in high growth markets, particularly as a new entrant, will be very different from the risks associated with more mature markets and therefore a separate risk assessment should be undertaken.

Another pillar in the prevention of fraud, bribery and corruption is the existence of a strong anti-bribery and anti-fraud culture, driven by clearly stated policies and high profile compliance activity. Having the right people in a high-growth market is key; people who understand and have experience of growing businesses in a responsible manner.

Employing local staff who come with a different set of engrained cultural values and using third party agents who do not operate to the same set of corporate ethical standards immediately leads to higher risk. As a result, it is difficult to overstate the need for training and awareness sessions to create and maintain the appropriate set of ethical values in a team operating in a remote high growth territory.

The importance of also performing appropriate background checks on key individuals and third party agents cannot be overestimated. Local intelligence in far flung places is a highly valuable commodity and our own Corporate Intelligence team often finds that the value of the insights gathered far exceeds the fees involved, if those insights prevent a disastrous decision in terms of new business partner or new local sales manager.

Detection

The key to detecting fraud, bribery and corruption in high growth markets is to apply rigour in terms of oversight, challenge and audit for compliance while having a good understanding of local business practices. If the risks are perceived as being higher, the compliance activity should be greater. Fledgling operations in high growth markets should fall within the scope of internal audit and third party contracts, for example with agents, should be audited regularly.

In addition, consistently exceptional performance, even in a high growth market, needs to be considered with an element of scepticism. If your regional team in a high growth market is winning significantly more than its fair share of contracts, this may be because bribes are being paid. If the value of contracts (debts and inventory) in progress on the balance sheet of your subsidiary in a high growth market is growing as a proportion of turnover and not matched by cashflow, this may actually indicate a problem in respect of financial manipulation to meet targets.

Additionally, keeping reporting lines open to allow communication of issues is key, as is responding promptly when there are suggestions that there may be a problem. In world class organisations, the approach to whistle blowing and the response to suspicions is consistent, regardless of where in the world the allegation arises.

“If the risks are perceived as being higher, the compliance activity should be greater.”

Focus on Fraud Risk in the IT Sector in India

India is one of the high growth markets where we have a long established Forensic practice. We have seen fraud and white collar crime increase over recent years – and the trend is likely to continue¹. In particular, the Financial Services sector is found to be the most susceptible to fraud, followed by Real Estate / Infrastructure and the Information Technology (IT) sector.

In India, in terms of IT, there are over four million highly trained English speaking technical professionals (second only to the USA). India has taken over the mantle of the software developer to the world. India exports software to 95 countries. According to a worldwide

survey, India is ranked as the most favourable destination for software outsourcing². Operations in India are of course a very different prospect than operations in for example the USA.

Whilst India does not score highly in the Transparency International Corruption Perceptions Index 2009, it is certainly not at the bottom of the list and its ranking is gradually improving. The Satyam accounting scandal in early 2009 showed that the IT industry in India is also susceptible to stock market driven accounting manipulation. This suggests that the risk focus should cover not only bribery and corruption issues but also sophisticated white collar criminality.

Investigation

Country-specific adjustments to fraud investigation mechanisms are an important consideration and should be influenced locally. Possible approaches involve setting out general principles, dos and don'ts about what actions to take, who should be responsible for the investigation, decision-making and reporting. An overarching fraud response plan clearly articulated for each region of business activity is a key requirement.

Yet research suggests that less than half of all companies have taken steps to protect against white-collar crime in foreign countries. According to research by KPMG International³, the majority, 56 percent, of companies surveyed are ill-prepared to investigate fraud promptly and effectively if it occurs in a country other than where they are headquartered. According to the study, they lack comprehensive protocols to cover the international investigation process.

“To do nothing about preventing, detecting and investigating cross border fraud is as good as an invitation to criminals. Unlike some corporates, they are unfazed by national boundaries”, says Alex Plavsic, KPMG's UK Head of Forensic.

60 Seconds with Ian Gomes, Partner, Head of High Growth Markets, KPMG

How does the economic crisis affect fraud and corruption in foreign markets and the fight of international investors against it?

In many cases this will be the first economic downturn businesses have experienced since entering into growth markets such as China, India or Vietnam. Continuous growth and favourable lending conditions may have helped mask some corporate deficiencies and even deliberate financial wrongdoing in the past. Increasing pressure on revenue, margins and liquidity invariably expose underlying problems in today's recessionary environment.

Are there any country-specific fraud or economic espionage risks in the crisis in high-growth markets?

Businesses must adapt their security strategies to reflect local legal and regulatory regimes. Risk aversion methods in one's own group headquarters might not be as effective abroad. In some high growth countries, foreign companies must disclose information and technical drawings to authorities and certification agencies in order to obtain product approval for the respective market. In some cases, there is a risk of innovative product knowledge falling into the hands of competitors. Forensic specialists anticipate economic pressure will boost such activities around the world.

What can companies do to safeguard their corporate secrets abroad during the current downturn?

The need for fast, reliable company information is heightened in times of crisis – especially for the assessment of balance sheets and the integrity of potential future business partners in an M&A environment. Companies may wish to scrutinise stakeholders more closely – especially joint venture, other business partners and suppliers in high-growth markets. How reliable are they in a crisis? What issues and pressures of their own are they facing? What recourse does the company ultimately have? Early detection measures can be vital – and banks and lenders see such risk provision as a key criterion, not least in a foreign market that is difficult to assess especially in these turbulent economic times.

What challenges and risks might arise from inside the company?

When times are hard, people may be more unscrupulous out of financial necessity. Intangible assets such as expertise, databases and technical drawings need to be protected. Disenchanted employees or those facing redundancy may be tempted to disclose sensitive data. Competitors and foreign secret services may be able to use these secrets to effect more aggressive and higher-risk activities.

Conclusions

An organisation should treat its ventures in high growth territories in the same way that it treats its core business activities. It should assess the fraud, bribery and corruption risks arising from its activities in that market and it should put in place the appropriate steps to prevent, detect and respond to the threats arising.

Even in high growth markets, our experience is that the most significant fraud risks come from within the organisation. The highly rated young executive, running operations on the other side of the globe, tasked with making rapid impact in a market where it is almost certain they will be offered inducements or asked for a bribe needs oversight, challenge and a clear framework within which to operate. If they are not given this support, should their employer really be surprised when faced with an allegation of fraud, bribery or corruption?

We would advocate that organisations identify their own vulnerabilities at the earliest possible stage, rather than waiting until they are added to the growing list of clients who fall victim to fraud or allegations of bribery and corruption, with the resultant loss in shareholder value. FF28



Alex Plavsic

Partner, Head of Fraud Services
KPMG Forensic practice in the UK
+44 (0) 20 7311 3862
alex.plavsic@kpmg.co.uk



Ken Milliken

Associate Partner
KPMG Forensic practice in the UK
+44 (0) 141 300 5857
ken.milliken@kpmg.co.uk



Brent McDaniel

Head of Anti-Bribery & Corruption
KPMG Forensic practice in the UK
+44 (0) 20 7311 3516
brent.mcdaniel@kpmg.co.uk

1 Source: KPMG India Fraud Survey Report, 2008
2 Source: www.bestweboutsourcing.com
3 Source: KPMG Cross-Border Investigations – Effectively meeting the challenge, 2007

6

5'6"

5

4'6"

4'



Roger Aldridge, Tom Russell and Tracey Wright from KPMG Forensic practice in the UK discuss work undertaken with law enforcement agencies throughout the UK.

The Role of Corporate Intelligence in Tackling Organised Criminality

Roger Aldridge

Tom Russell

Tracey Wright

Background – The Development of Forensic Accounting in Law Enforcement

Forensic accountants carved out a niche for themselves in the accountancy profession in the late 1980s and 1990s. The leading role played by the early forensic accountants in a number of high profile investigations for the Bank of England, the DTI, the FSA and other regulators cemented that specialism. Subsequently, many large accounting firms have developed sizeable "Forensic Accounting" departments, employing accountants and other professionals working to help clients investigate allegations of fraud and misconduct, dealing with regulatory issues, tracing assets and providing expert evidence in Court. Law enforcement agencies lagged behind somewhat in the use of forensic accounting skills in relation to fraud and financial crime investigations. However we have seen significant change in recent years, with the value of forensic accounting input now generally accepted across the law enforcement community. At the same time, the range of skills within Forensic teams in the accountancy profession has been further extended to include economists, technology specialists and corporate intelligence specialists.

This experience has created a significant, effective and professional fraud investigation capability in most large accountancy firms which we are increasingly offering to law enforcement agencies. The service essentially falls into three areas of expertise,

- expert witness; providing analysis of financial data leading to an expert view as to any criminality involved;
- technology support and analysis; all investigations these days involve the gathering of large amounts of data from differing sources, and being able to quickly analyse that data to identify the key evidence is key; and
- 'corporate intelligence' or the accessing of 'hard to reach' open source data required to have a complete understanding of the financial picture. In this article we will concentrate on this latter area.

Corporate Intelligence

The darker side of human nature is a reassuringly reliable source of employment for both law enforcement practitioners and civil investigators. Whether bad, or weak, or arrogant, there will always be people who, for private gain, are tempted to break

the law; and while the criminal justice system may attempt to address society's demand for punishment by means of appropriate sentencing, a more enduring and difficult challenge often remains once the cell door has clanged shut: how to ensure that the proceeds of the criminal act are identified and recovered.

As crime and criminals have become increasingly sophisticated, so too have their efforts to conceal money and assets beyond the reach of law enforcement, despite existing anti money laundering legislation and recent moves by regulatory authorities around the world to tighten the rules affecting offshore jurisdictions. It remains relatively simple for criminals to hide behind the minimal disclosure requirements of so-called 'tax havens'. Even with court-appointed or law enforcement powers, identifying beneficial ownership or associated bank accounts can be a lengthy and frustrating process; and, of course, by the time one has fought one's way through the thickets of procedure and bureaucracy, the assets may have been moved on again, necessitating another round of forms and applications.

“What the use of fingerprints was to the 19th century, and DNA analysis was to the 20th century, so financial information and forensic accounting has come to be one of today’s most powerful investigative and intelligence tools available in the fight against crime and terrorism.”

The Rt. Hon. Gordon Brown MP, in a speech on
“Meeting the terrorist challenge” given to Chatham House,
10 October 2006

These evident vexations aside, there are ways to move more effectively against known or suspected assets. The increasing trend for government agencies in many jurisdictions around the world to digitise publicly available information databases and property registers means that certain assets are becoming quicker – if not necessarily easier – to identify. Nevertheless, certain barriers remain: ‘Where do I go to find out about company ownership in France?’, for example; ‘Are Spanish property records held locally or centrally?’, ‘How much does it cost to access this type of information?’. Unless one makes regular use of such material, keeping on top of the latest developments in data-gathering and information organisation is not only time-consuming but has lately become more and more expensive: governments and providers are aware that the information they hold is a valuable commodity.

It is in this area that co-operation between law enforcement authorities and civil investigators can be most valuable. KPMG’s Corporate Intelligence team not only has access to dozens of databases covering many different types of information across multiple jurisdictions, but also holds knowledge of precisely what material is available in which territory and under what circumstances.

A Recent Request for Help

Our client, a creditor of a UK individual living in Spain had information that the subject owned property and other assets in Spain. We were able to establish the subject’s residential

history in Spain by identifying past registration of a vehicle in the subject’s name. Armed with this information, we conducted enquiries at the Commercial and Land Registries in Spain, where we identified five houses of which the subject was the sole proprietor and on which we were able to establish the properties’ mortgage status (both the amount of the charge and the bank holding the charge). One of the larger properties was found to have been pledged as collateral to a Spanish-registered company in return for the majority of that company’s shares. In addition, information from the Property and Mercantile Registrars and the Spanish commercial registry found three further companies in which the individual held an interest. The information gathered enabled our client to take steps to recover the money which the subject owed.

Using the same process in complex criminal cases can quickly open up new lines of formal inquiry by law enforcement agencies.

Of course, it is unfortunately not always possible to guarantee results on every occasion – as mentioned before, criminals can be adept at concealing assets – but with the right partner with the necessary knowledge, the process can at least be simplified. FF29



Roger Aldridge
Director
KPMG Forensic practice in the UK
+44 (0) 20 7694 5542
roger.aldridge@kpmg.co.uk



Tom Russell
Senior Manager
KPMG Forensic practice in the UK
+44 (0) 20 7694 5527
tom.russell2@kpmg.co.uk



Tracey Wright
Manager
KPMG Forensic practice in the UK
+44 (0) 121 609 5911
tracey.wright@kpmg.co.uk



Fighting Fraud in Nigeria – What Progress has been Made?

Steven Haynes

Public perceptions of Nigeria are generally negative. Nigeria is synonymous for many with fraud and financial crime, including bribery and corruption. Yet Nigeria has made great efforts in recent years to tackle fraud, corruption and governance failures, even if existing perceptions are so entrenched that they will take many more years to change. Steven Haynes, Head of KPMG's Corporate Intelligence service in EMEA, looks at a recent 'shake-up' of the Nigerian banking sector, considers how best to evaluate Nigeria's efforts at fighting fraud and corruption – and what this means for European companies investing or trading with Nigeria.

In August 2009, the Central Bank of Nigeria (CBN), led by its newly appointed governor Sanusi Lamido, sacked the chief executives of five Nigerian banks and ordered investigations into their activities. Criminal investigations are also underway into several of the former bank chiefs. The banks are accused, inter alia, of having built up excessive portfolios of non-performing loans due to lax corporate governance and credit risk management. They also lent money to clients so that these clients could buy the same banks' shares. This bubble has now burst, leaving a slew of non-performing loans. The governor also announced a N400 billion (\$2.6 billion) capital injection to enable the banks to continue trading under new management. In taking

this action the CBN shed light on what some critics have long viewed as a poorly managed sector suffering from inadequate controls and oversight.

According to the CBN the five banks collectively held non-performing loans worth a total of N747 bn (\$4.9 bn) representing almost half of all lending by those banks. The CBN also published a list of major bank debtors. Containing over 200 names, it included some of Nigeria's best known business figures and their companies. (NB. Many on the list have claimed that the CBN's data is inaccurate).

The five banks most affected are Oceanic Bank, FinBank, Afribank Nigeria, Union Bank of Nigeria and Intercontinental Bank. These are not inconsequential banks. They emerged from the 2006 banking consolidation in Nigeria, which saw the number of banks reduced from 89 to 25. They advertised internationally, garnered prizes from banking magazines and were energetic corporate sponsors. Two of the five banks have operations in London regulated by the UK's Financial Services Authority (FSA). One of the chief executives now under criminal investigation was authorised by the FSA at the time of his arrest in Nigeria.

In parallel with the CBN's actions, criminal investigations were launched by Nigeria's Economic and Financial Crimes Commission (EFCC). Four of

the five bank executives were arrested. The fifth is suspected of having fled to London and is accused of transferring approximately £10 million belonging to his bank to a UK law firm. In January 2010, a UK court granted a worldwide injunction against the former executive in favour of the bank. At the time of writing, the EFCC confirmed that all five former bank executives are facing multiple criminal charges, including of fraud and money laundering.

The EFCC, established in 2002, is Nigeria's lead anti-fraud agency. It has notable achievements, investigating, convicting and jailing major criminals behind advance fee frauds and other scams.

The EFCC has also taken action against many of Nigeria's powerful state governors, who control huge budgets. At one point in time, the majority of Nigeria's 35 governors were under investigation for alleged corruption. These high-profile investigations, whose progress was closely followed by international governments, regulators and NGOs, signalled that Nigeria was making tangible progress to tackle fraud and corruption, and thereby slowly changing perceptions among prospective business partners.

However, Serious Challenges Remain

First, the EFCC itself is widely perceived to have lost ground in the last two years. In December 2007, the EFCC arrested the most powerful of the state governors on suspicion of corruption on a huge scale. (Two international oil companies were publicly embroiled in some of the alleged corruption). But within days, the energetic head of the EFCC had been removed. The case against the governor (who had also been under investigation by the Metropolitan Police) stalled. Since then, many observers contend that the agency has lost its bite. The investigation and prosecution of fraudsters, including those targeting US and European nationals, continues; but the agency's anti-corruption efforts are perceived to have been blunted by political compromises and legal challenges in a judicial system lacking independence.

Second, cooperation between Nigeria's law enforcement agencies and its international counterparts is patchy. Millions of dollars plundered by the late military leader Sani Abacha (who died in 1998) were effectively laundered by British banks in London. Privately, the Nigerian authorities consider the

UK authorities to have been lukewarm in their efforts to identify the money flows and assist the repatriation of stolen funds. On the British side, the Metropolitan Police was reportedly frustrated in the lack of cooperation from the former Nigerian Attorney General in its own investigations of allegedly corrupt state governors with strong UK ties. Cooperation on criminal cases with a political dimension is more delicate than purely criminal cases.

Third, with political factors playing a part in the high-profile cases, Nigeria's current political uncertainty makes predictions for the direction of anti-fraud and corruption efforts difficult. In February 2010, Vice President Goodluck Jonathan became acting president, following the prolonged absence of President Umaru Yar'Adua, who died in May. The leadership vacuum caused rifts within cabinet, heightened volatility in the oil-producing Niger Delta and threatened a constitutional crisis. Jonathan's immediate demotion of the controversial Attorney-General and Minister of Justice yet again changes the landscape in which fraud and corruption will be tackled.

Indeed, the political changes have already led to dramatic changes in the law enforcement landscape. In mid-May, the most powerful of the former state governors accused of corruption, whose prosecution looked to have stalled for so long, was arrested. He may be extradited to Nigeria or to the UK, where British police wish to question him over suspicions that millions of pounds of suspect funds passed through British banks and was invested in London. For the time being, the EFCC is firing with all guns blazing once again. And the strong connections between alleged financial crime in Nigeria and the UK may be demonstrated as never before.

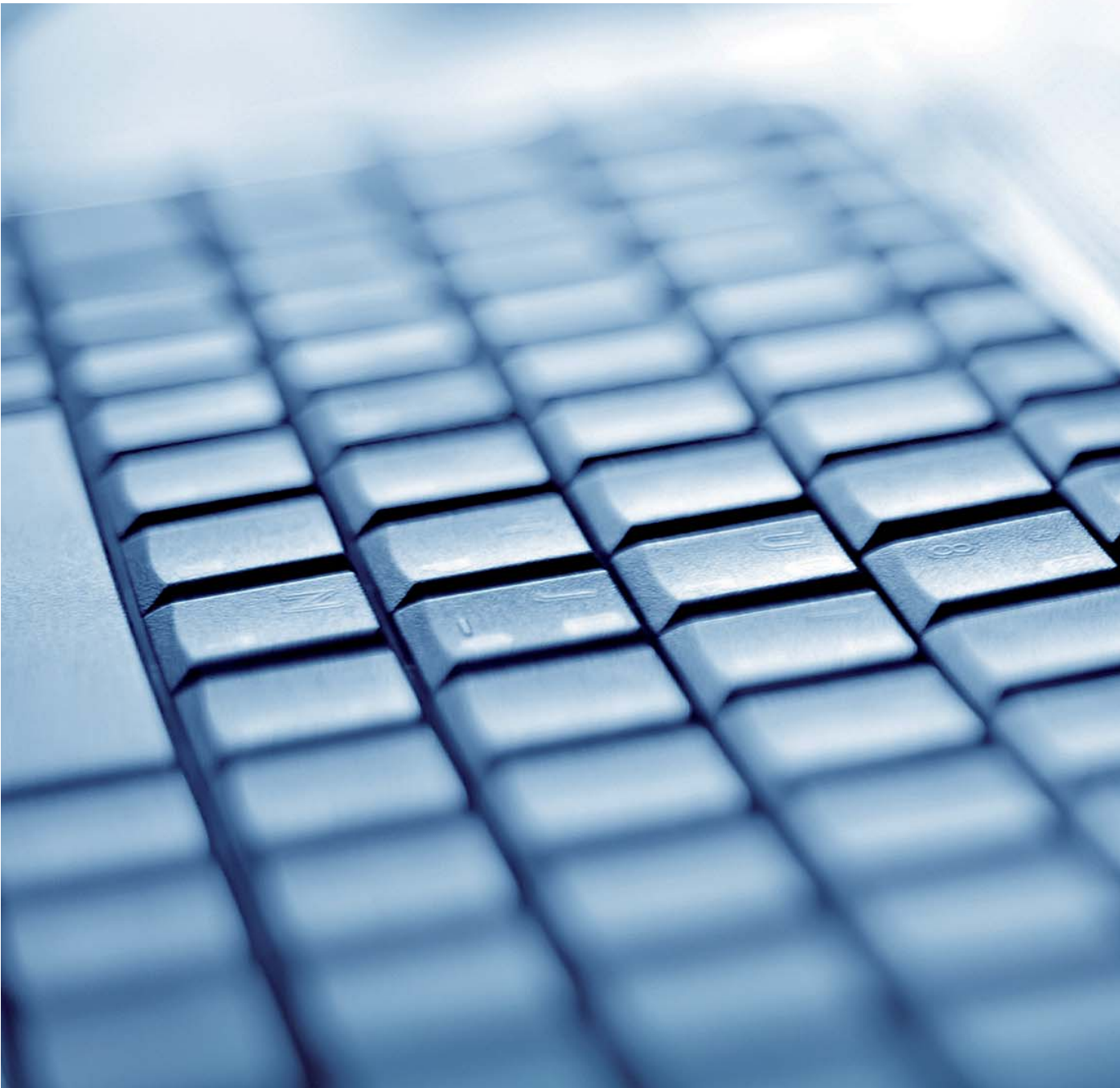
In summary, Nigeria has made considerable progress in tackling "industrial scale" fraud and much advance fee fraud and other scams are now coordinated by Nigerians in other countries. The EFCC's early efforts against corruption won some international admiration, even if the agency's revelations have simultaneously reinforced existing perceptions. Much now depends on the attitude of the new Attorney General and the extent to which the EFCC will be free to take on powerful, vested interests.

Some Sensible Precautions when Considering Business in Nigeria:

- The CBN publishes the names of companies and individuals holding non-performing loans with the five worst affected Nigerian banks. Caution should be exercised when dealing with entities on this list. The anti-corruption authorities are co-operating closely with the CBN and criminal investigations may follow.
- Allegations of wrongdoing are frequently and publicly made in Nigeria. Newspapers are corrupted to publish scurrilous or inaccurate claims to further the interests of their owners or other parties. Such allegations should be verified, to the extent possible, and placed within a wider business or political context.
- Be alert to the possibility that the people with whom you are dealing could be 'fronting' for other parties including politically exposed persons.
- Ensure you understand the banking relationships held by your counterparties. In particular whether your counterparties are obtaining financing from non-arms length banking relationships.
- Allegations of corruption and fraud may be energetically investigated by the Nigerian authorities. Compared to other emerging markets, these investigations are usually widely reported in the local media. Consequently, for investors associated with those under investigation, the risks of negative public exposure are heightened. FF29



Steven Haynes
 Director, Head of Corporate Intelligence
 KPMG Forensic practice in the UK
 +44 (0) 20 7694 5390
steven.haynes@kpmg.co.uk



For German companies conducting fraud investigations, the search for relevant electronically stored information has become a central part of the investigation procedure. In the modern business world, a fraud investigation should not only involve the analysis of financial data, but also the analysis of key employees' communication (e.g., e-mails, SMS, instant messaging, voice recording) and working papers (e.g., office documents and pdf files). Yet, how much of this is legally possible in Germany, and how is it done?

The Use of Forensic Technology in Investigations in Germany – Legal Barriers and Technological Potential

Helmut Brechtken

Tom Hopkinson

Thomas Fritzsche

Personal data, such as e-mails of the relevant employees, can be a key element in a fraud investigation. However, there are potential barriers to accessing this information within German legislation and jurisdiction. When planning to collect e-mail data, attention should be paid to the possibility that employees' e-mails could be protected by the secrecy of telecommunications under article 88 of German Telecommunications Act (Telekommunikationsgesetz, TKG). This is the case if private use of the companies e-mail system is permitted – or at least tolerated – and the telecommunication has not yet been sent to the recipient. Many of our German clients do indeed allow private use of the company's e-mail system or are at least tolerating it under the terms of the Act. A company 'tolerates' private use if the prohibition of private use is not communicated and controlled continuously or the management knows about the private use and violations are not punished. Consequently, the company is prohibited from disclosing the content of communication to its management or third parties if it goes beyond the mandatory content necessary to provide the e-mail service.

It is important to note that protection by secrecy of telecommunication ends the moment the e-mail reaches the recipient. According to the Federal Constitutional Court (Bundesverfassungsgericht, BVerfG), secrecy of telecommunications shall continue as long as the e-mail is saved on an external provider's mail server, since it is accessible by third parties. In fact, every major corporate

email system saves email data on its servers. Intervention in secrecy of telecommunications is legitimised under certain limited conditions. It is still a controversial area as to whether suspicion of criminal activity by an employee represents a valid condition.

In any forensic technology exercise, electronically stored information may have to be collected, preserved, processed, reviewed and presented on the basis of specific criteria, and in a specific way, to make the information admissible in court. The documents may be located on servers, desktop computers, notebooks, smartphones, and other communication/storage media. Besides collecting evidence related to the facts of the case, the real challenge is identifying and disclosing all relevant documents within a potentially very large pool of corporate information, normally using a widely dispersed search pattern and under substantial time pressure.

A central aspect in this process is the utilisation of specialist forensic technology software which processes and filters the data as well as provides the review platform. The features of these software solutions have a different focus and application depending upon the circumstances of the investigation.

How can Forensic Technology Software Help to Detect Fraud?

We consider this question below by analysing one of the crucial steps in the process, namely data filtering.

Normally there is a specific timeframe during which each suspicious event

or alleged fraudulent activity has taken place. Furthermore, there are a certain number of individuals of interest whose e-mail accounts and other media will have to be collected and evaluated. For the purposes of completeness, it might be an option to review the complete e-mail traffic of the suspects within the respective time frame. When dealing with manageable data volumes, this approach may be feasible in terms of detecting whether a fraud has taken place. In a case involving several gigabytes or terabytes of data (i.e., the paper equivalent of millions of pages), there has to be an element of data filtering in order to create a manageable volume of data to review.

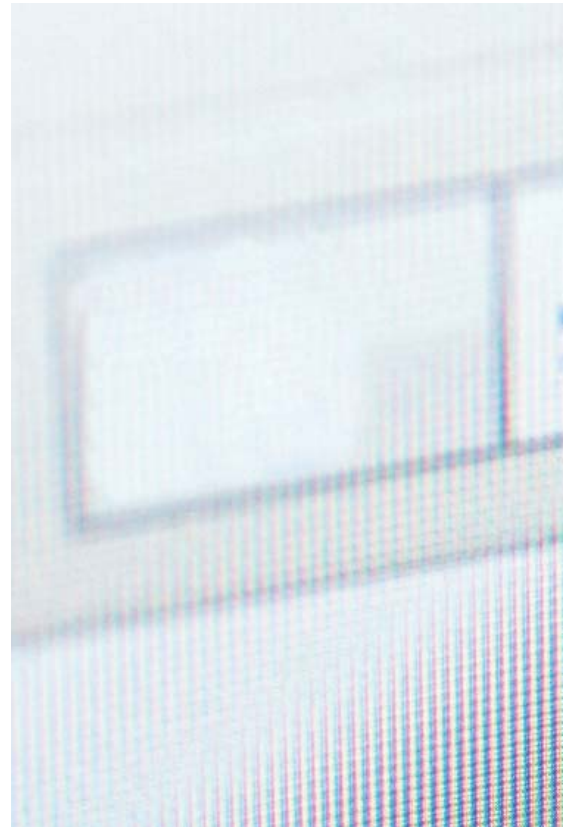
The following filtering measures are particularly effective for the elimination of irrelevant documents:

- Deduplication of documents
- Focusing on specific file formats (e.g., .msg, .nsf, .doc, .pdf)
- Focusing on a certain period of time as regards e-mails
- Focusing on specific persons (addressee / addresser of e-mails)

However, the result of this relatively simple procedure may mean that a substantial volume of documents will still need to be reviewed. At this point, a more complex area of data filtering by keywords can be used. But in the context of a fraud investigation, the real challenge may be how keywords and other methods can be used to look for evidence that relates to the

“Protection by secrecy of telecommunication ends the moment the e-mail reaches the recipient.”

“Fraudsters are likely to have ‘covered their tracks’ in the language they use to communicate with each other.”



fraudulent activities that are typically hidden or more difficult to find within the data. In other words, which keywords should be used if one does not know at the outset all the details about the fraudulent act, the persons involved, or the words and phrases that the fraudsters are using in their communications?

The following examples illustrate how forensic technology software can help in these scenarios.

- In a **statistical evaluation of a suspect’s e-mail communication**, the software lists all persons or email addresses that an individual contacted within the period under investigation. It also states the number of e-mails sent to or received from another person. It is often the ‘rare’ communications which are interesting, as employees who know each other often exchange hundreds, even thousands, of e-mails.
- Another useful function to help refine a keyword list is the **listing of words of similar orthography (keyword suggestion)**. Here, the investigation team creates a list of keywords – for example a compilation of names of known persons and companies and certain

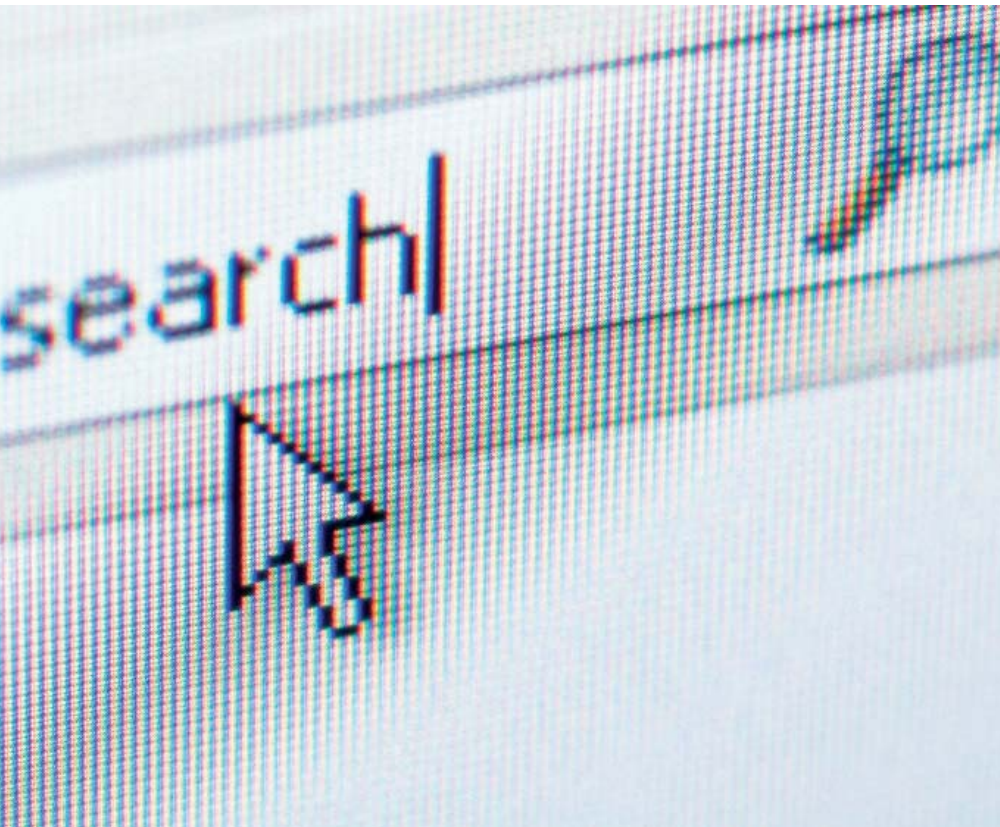
words, adjectives, account names etc., that might have been used. These are then applied to the saved e-mails by means of various filtering options. The results show the respective number of e-mails containing a specific keyword or phrase which can then be reviewed. Furthermore, the software also lists words similar to the keywords. If they appear ‘interesting’ with regard to the potential sequence of events, they can easily be added to the keyword list. The keyword list is thus repeatedly refined, normally leading to an optimised set of results.

- A third solution operates as a **learning system**. A certain number of e-mails are subject to a linear review (i.e., reviewing one after another). Having analysed and categorised 2,000 e-mails, for instance, into the classes ‘relevant’ and ‘irrelevant’, the software analyses the keywords in the e-mails according to certain statistic processes (e.g., frequency of occurrence and interval of words). On this basis, the software makes ‘suggestions’ about how to categorise those e-mails which have not yet been reviewed. This method is a good way to quickly gain an insight into potentially relevant e-mails and to deepen the

understanding on the sequence of events, if the initial situation is unclear and if the data volume is too large to review all documents.

- Another type of software uses **document visualisation**. It presents the e-mails to be reviewed in a visual, two-dimensional format. Typically, one ‘dot’ on the screen represents a document, and similar or identical documents are grouped and shown in a cluster. The critical keywords of the group which have been identified by the system are also indicated. This method permits a quick analysis of e-mails, as the two-dimensional presentation appears to be particularly ergonomic for the human perception. The use of this type of visual software is often highly valuable when large volumes of data need to be reviewed under tight deadlines.

These examples clearly show the importance of being able to offer the most appropriate forensic technology software depending on the specific requirements of an investigation. The individual software solutions are many and varied, as are their functions. It takes both time and people to understand and evaluate them.



Helmut Brechtken
Senior Manager
KPMG Forensic practice in Germany
+49 221 20 73 5848
hbrechtken@kpmg.com



Tom Hopkinson
Senior Manager
KPMG Forensic practice in the UK
+44 (0) 20 7694 5304
tom.hopkinson@kpmg.co.uk



Thomas Fritzsche
Assistant Manager
KPMG Forensic practice in Germany
+49 173 5600557
tfritzsche@kpmg.com

e-Disclosure in Action – A Case Study

The legal challenges described above were illustrated clearly in a recent investigation carried out by KPMG Forensic practice in Germany. Within the company in question, although the private use of the corporate e-mail system was technically prohibited according to the IT policy, the sending of private e-mails was tolerated by the management in practice. The strategy in the first phase of the investigation was not to inform the suspected employees; therefore, asking them for consent to access their e-mails for the purposes of data analysis was not an option and performing an e-Disclosure exercise at that time was not possible. However after four weeks of investigation, in which hard-copy documents and database information were analysed, and the fraud methodologies became more traceable, the decision was made to inform the suspects about the investigation.

At this stage they were asked for consent to access their e-mails, which all agreed on. Now, the challenge was to analyse the relevant laptops, e-mail accounts and smart phones of the relevant employees within just one week (the deadline set by the executive board). Based on the knowledge of the case built over the previous four weeks – along with technical skills and previous experience – the investigation team developed a tailored e-Disclosure methodology. By applying some sophisticated specialist software, we were able to identify and separate a small number of highly relevant e-mails from a total pool of 350,000 documents (representing approximately 40GB). When faced with the e-Disclosure findings in interviews, the five relevant employees admitted to their fraudulent actions. FF29

Cases in Point

A selection of case studies from across a range of sectors and territories



Case Study 1: Dodgy directors disqualified through teamwork of KPMG/Companies Investigation Branch (CIB)

October 2009 saw the disqualification for 12 years of two Swiss-based company directors who deceived UK investors into paying more than £5m in a 'land-banking' scam. The land banking company (now in liquidation) bought land for just over £600,000 and then sold nearly 750 plots to the investors for £5m. Investors were told that the land would receive planning consent for development and would increase dramatically in value. That permission was never granted and the plots have remained undeveloped.

The CIB launched a full investigation into the land banking company following the receipt of a complaint. KPMG Forensic practice seconded a manager to the CIB for one year who participated as part of the core investigations team.

On 30 October 2009, the former Directors signed disqualification undertakings after the CIB investigation revealed a pattern of unfit conduct. The individuals accepted that their misconduct made them unfit to be company Directors, acknowledging that they had:

- Failed to give any or any proper consideration to the legality of the company's land-banking scheme;
- Caused or permitted unfounded and misleading statements to be made to the public in connection with the plots of land;
- Caused or permitted the company to enter into voluntary liquidation in Switzerland without making any provisions to refund money to UK investors; and
- One of the directors admitted misrepresenting the company's scheme to the Financial Services Authority.

Business Minister Ian Lucas commented on this case saying "This sends a strong message to company directors who deceive and rip-off members of the public: we will investigate and take firm action against you." He added "Investors should also be wary of any land-banking or other schemes which promise huge profits for little outlay. To use the old adage, if it sounds too good to be true, it probably is."¹

“The Individuals accepted that their misconduct made them unfit to be company Directors.”

¹ <http://www.ftadviser.com/FTAdviser/Regulation/Regulators/Treasury/News/article/20091030/94a23f88-c53d-11de-b1d4-00144f2af8e8/Two-directors-disqualified-over-5m-scam.jsp>

Case Study 2: Identification of theft leads to criminal conviction

Our firm's client – a large life insurance company – performed its own internal investigation into allegations of theft of a policyholder's assets. The investigation found that 51 payments totalling approximately £540,000 were suspected of being diverted over a six year period by a long serving female employee. The police were informed of the situation and the employee suspected of being involved in the alleged diversion was arrested, interviewed under caution, and released on bail.

KPMG was engaged by the client to evaluate the adequacy of the investigation already undertaken and assess whether the client's evidence supporting the allegation was appropriate and sufficient. We were also asked to assist the client establish additional facts behind the suspect's ability to manipulate electronic payment details.

As part of the investigation we conducted a series of interviews of current employees to gain an understanding of the claims management process. We learned that a combination of user identification and password was required to operate the administration and payment system and that it was common practice for staff to keep written records of their log-in details in various unsecured locations.

Our investigation also involved the use of data analytics to identify trends in the suspect's behaviour. These observations were translated into detection rules which were applied to over one million transactions in various claims data systems covering several years. We confirmed that twelve bank accounts, all either in the name of or under the control of the employee, the employee's step-father or mother, were used by the suspect to divert the 51 payments. Negligent behaviour around

information security and poor IT systems and controls allowed the suspect access to the unattended computers of her colleagues and to request and approve a change in bank details during the claims management process.

We also identified over 13,000 additional potentially suspicious transactions with an estimated value of £70 million for possible further investigation by the client.

The suspect was charged with theft and the suspect's mother and step-father were charged with 'concealing criminal property' and 'money laundering' under the Proceeds of Crime Act.

Case Study 3: KPMG in the Netherlands and KPMG in Kenya collaborate to unveil corruption

Our firm's client, a global not-for-profit organisation that provides medical supplies to economically underdeveloped countries, received allegations of irregularities in its purchase-to-pay process at one of its African subsidiaries. A change in local management led to claims that certain company employees had received nearly €30,000 in kickbacks and €60,000 in cheque payments made to entities owned by these individuals.

Our firm's client – a Dutch based company – engaged KPMG Forensic practice in the Netherlands to perform an investigation into the allegations to identify the individuals involved in the purported scheme and assess the level and extent of any irregularities in the purchase-to-pay system. Our work was carried out considering Dutch laws and regulations, which required the assistance of KPMG in Kenya in notifying in person the four individuals of interest at the outset of the engagement of their suspected involvement.

KPMG in the Netherlands, in conjunction with KPMG in Kenya performed interviews of the subjects and a review of the purchase-to-pay system. Our work revealed instances where information contained in the purchase-to-pay system was inconsistent with accounting systems data, incomplete, and/or unsupported by relevant hard copy documentation. It also indicated that costs had been recorded in the clients' accounting system based on potentially fake invoices or invoices with inflated prices issued by supplier companies in which the suspect individuals held an interest as director and/or shareholder.

We attempted to present our observations in a face-to-face meeting with each subject to allow them the opportunity to respond. Two of the individuals attended the requested meetings whilst the other two declined. This uncooperative behaviour led the client to initiate its own direct enquiry of the subjects as to whether they had any interest in suppliers of the organisation. Three of the four individuals acknowledged such interest and were subsequently dismissed.

At the conclusion of our work, KPMG provided the client with a fact finding investigation report and a supplemental report detailing recommendations for improving its purchase-to-pay process. The client commented that they were very pleased with our investigation strategy throughout, the clarity with which our investigations procedures were executed, and that they planned to perform a global review of their purchase-to-pay process as a result of our work.

Case Study 4: Opportunity and incentive lead to fraud

An international Swiss based client became aware of unusual payments being made out of its Swiss bank account into foreign bank accounts and notified authorities, initiating a criminal investigation. A senior level employee was identified as the main suspect and was arrested. Upon questioning, the suspect admitted to taking 'some money' and was subsequently dismissed. KPMG Forensic practice was then engaged by the client to perform an independent investigation, quantify the extent of the loss, and gain an understanding as to how the unauthorised payments were made.

Performing our investigation in accordance with Swiss law and regulation, we conducted interviews of selected company employees to gain a thorough understanding of the company's electronic bank payment software system and processes; obtained images of electronic payment files which we reviewed quickly and accurately with the assistance of our Forensic technology specialists, and used corporate intelligence capabilities to perform a background check on the former employee and his close relatives in Switzerland and abroad.

Our investigation revealed that weaknesses in the client's bank payment software system and lack of segregation of duties allowed the suspect to defraud the company. In his role, the suspect was responsible for maintaining the bank payment software system (which provided him with 'super user' rights) and for approving requested payments. This combination permitted the suspect to initiate and approve 20 unauthorised payments totalling approximately €1.5m.

We completed our work and reported our findings to the client in sufficient time for the client to obtain a notarised repayment declaration from the former employee which required the individual to reimburse the company for the full value of the defrauded amount. Further, the result of our work heightened our client's awareness of similar potential weaknesses at other locations and prompted the client to implement a global review of its banking payment systems and processes.

FF29

“Weaknesses in the client's bank payment software system and lack of segregation of duties allowed the suspect to defraud the company.”

“Review team was able to prove the client’s suspicions of improper payments and to identify the individuals involved.”

Case Study 5: e-Disclosure used to turn a mountain into a molehill

Our firm’s client – a global manufacturing company—engaged KPMG’s Forensic Technology practice (FTech) to assist with their investigation into alleged improper payments between subsidiary companies and third parties located across three separate European jurisdictions. The investigation required FTech to research and identify potential data sources in all jurisdictions and provide the investigation team and the client’s lawyers with potentially relevant documents for review within three weeks.

We worked closely with the client and its lawyers to understand possible data sources and to plan the collection phase and processing requirements. The data sources identified were located across Central and Eastern Europe, which required us to take various data privacy restrictions into account. A joint UK and Russian team commenced with the collection phase on-site within 24 hours of being instructed. The team liaised with the client and its local in-house counsel to overcome the data privacy and data protection challenges, whilst collecting the data in a forensically-sound manner. Within 36 hours we had transferred 1.6 terabytes of data to KPMG’s Forensic DataLab™ in the UK for culling and processing. Through use of SFTP (secure file transfer protocol) sites much of the data was transferred immediately upon collection to provide the review teams with instant access.

By using a number of sophisticated software review tools, we were able to cull the initial data set from circa 1.3 million documents to circa 61,000 documents – five percent of the original source. The culling process involved the removal of common system files, specific file types, duplicates and near duplicates before entering the data into an e-disclosure review tool. A date range and specific search terms relevant to the case were then applied to reduce the data further. We then used a concept-mapping tool to search for specific nouns and concepts across the data. By ‘understanding’ the language used, the review tool was able to cluster documents deemed as potentially relevant to the investigation which enabled the client to focus on relevant material quickly.

One of our e-disclosure professionals provided training to our client and helped them develop their review strategy. We also provided 24/7 technical support throughout the engagement to ensure the client could meet the deadline. Our processes provided the client with a cost effective solution to quickly identify relevant data and allow the investigation team to have access within a very tight time frame.

As a result of our work the review team was able to prove the client’s suspicions of improper payments and to identify the individuals involved. Our client was able to take legal action against those individuals and renegotiate specific contracts with its third parties to obtain better trading conditions going forward with improved controls.

Without FTech’s methodology and forensic tools, our client would not have been able to meet the deadline set and quickly identify documents to act upon in this particular investigation. We saved our client a substantial sum of money with the culling approach that was taken and the expert training provided; which drastically reduced the time our client’s lawyers spent on the review.



Acknowledgements

Thanks should go to the following people who contributed to the drafting and production of this issue of *Fighting Fraud*.

Tammie Davis
Sabina Joseph
Laura Klysz
Edward Palmer
Madeleine Rebsamen
Matt Congreve
Darren Pauling

Emma Quinn
Jonathan Froome
Gus MacKenzie
Martijn Hin
Katarina Kurtin
Matt Jackson
Dirk Zander

KPMG in the UK

Adam Bates
Tel +44 (0) 20 7311 3934

Jeremy Outen
Tel +44 (0) 20 7311 3861

Hitesh Patel
Tel +44 0 20 7311 3571

Alex Plavsic
Tel +44 (0) 20 7311 3862

Richard Powell
Tel +44 (0) 161 246 4044

KPMG in Argentina

Geronimo Timerman
Tel +54 11 4316 5980

KPMG in Australia

Gary Gill
Tel +61 (2) 9335 7312

KPMG in Austria

Gert Weidinger
Tel +43 732 6938 2107

KPMG in Belgium

Els Hostyn
Tel +32 (0) 2708 4362

KPMG in Brazil

Jose Carlos Simoes
Tel +55 11 3245 8383

KPMG in Canada

Jim Hunter
Tel +1 416 777 3193

KPMG firms in Central and Eastern Europe

Jimmy Helm*
Tel +420 222123 430

KPMG in Greater China

Grant Jamieson
Tel +852 3121 9804

KPMG in Denmark

Torben Lange
Tel +45 3818 3184

KPMG in France

Jean-Luc Guitera
Tel +33 (0) 1 5568 6962

KPMG in Germany

Frank Weller
Tel +49 89 9282 1050

KPMG in India

Deepankar Sanwalka
Tel +91 124 3074302

KPMG in Ireland

Laura Burge
Tel +353 (1) 410 2768

KPMG in Italy

Gabriella Chersicla
Tel +39 02 6763 2440

KPMG in Japan

Toshifumi Takaoka
Tel +81 (3) 5218 6725

KPMG in Korea

Kyong Choul (Chris) Shin
Tel +82 (2) 2112 0788

KPMG in Luxembourg

Eric Collard
Tel +352 22 51 51 7240

KPMG in Malaysia

KimChuan Tan
Tel +60 (3) 7721 3388

KPMG in Mexico

Shelley Hayes
Tel +52 55524 68300

KPMG firms in the Middle East

Roy Muller**
Tel +971 (4) 424 8900

KPMG in the Netherlands

Jack de Raad
Tel +31 10 453 4162

KPMG in Nigeria

Linus Okeke
Tel +234 (1) 463 0291-3

KPMG firms Offshore Financial Centres

Michael Fayle***
Tel +44 (0) 1624 681043

KPMG in Russia and CIS

Ian Colebourne
Tel +7 (495) 937 2524

KPMG in Singapore

Bob Yap
Tel +65 62132677

KPMG in South Africa

Herman de Beer
Tel +27 11 647 7342

KPMG in Spain

Pablo Bernad
Tel +34 91 456 3400

KPMG in Sweden

Martin Kruger
Tel +46 (8) 723 9199

KPMG in Switzerland

Anne van Heerden
Tel +41 44 249 3178

KPMG in the US

Richard Girgenti
Tel +1 (212) 872 6953

* **Home firm:**
KPMG in the Czech Republic

** **Home firm:**
KPMG in the United Arab Emirates

*** **Home firm:**
KPMG in the Isle of Man

The information contained herein is of a general nature and is not intended to address the circumstances of any particular individual or entity. Although we endeavour to provide accurate and timely information, there can be no guarantee that such information is accurate as of the date it is received or that it will continue to be accurate in the future. No one should act on such information without appropriate professional advice after a thorough examination of the particular situation.

The views and opinions expressed herein are those of interviewees and do not necessarily represent the views and opinions of KPMG LLP (UK).

© 2010 KPMG LLP, a UK limited liability partnership, is a subsidiary of KPMG Europe LLP and a member firm of the KPMG network of independent member firms affiliated with KPMG International Cooperative, a Swiss entity. All rights reserved.

KPMG and the KPMG logo are registered trademarks of KPMG International Cooperative, a Swiss entity.

Designed and produced by KPMG LLP (UK)'s Design Services

Publication name: Fighting Fraud Issue 29

Publication number: RRD-177861

Publication date: June 2010