



FORENSIC

Fighting Fraud

Issue 23 Summer 2007

ADVISORY

Contents



3

**US State Reporting Requirements
for Healthcare Professionals**

Simon Tottman
Hitesh Patel

7

**Tracing and Recovering Stolen Funds:
The Civil Approach**

David Hilton

10

**Fraud, Money Laundering and the
Insurance Industry**

David Hicks
Jonathan Peake

14

**A Practising Manager's Primer
on Handling Fraud Investigations**

Arvind Chopra

17

**White Collar Crime:
The Electronic Avenue**

Paul Tombleson
Georgina Lewis

US State Reporting Requirements for Healthcare Professionals

Simon Tottman

Hitesh Patel

Simon Tottman and Hitesh Patel from KPMG Forensic examine a growing US initiative aiming to achieve greater insight into the type of, and reasons behind, pharmaceutical company expenditure on healthcare professionals (HCPs).

Although the drive for the state reporting requirement is coming from US authorities, this level of scrutiny is likely to put firmly on the agenda of senior pharmaceutical executives potential issues of fraud and misconduct, either in collusion with HCPs or by employees diverting resources for a personal gain.

A background of greater industry scrutiny and regulation

Pharmaceutical companies are under increasing pressure in the US and Europe to be more open about their sales and promotional activities as government agencies look to drive down expenditure on drugs. In 2005 the US pharmaceutical industry spent \$11.4 billion on promotional activity, predominantly targeted at HCPs¹. Meanwhile, between 1994-2006 US retail prescription prices rose at almost triple the average annual inflation rate².

Regulatory bodies want to ensure HCPs are not improperly influenced by marketing and that payments, services, trips and other activities conducted with HCPs are appropriate. At the same time, pharmaceutical companies are under increasing pressure to deliver growth within an environment of pricing pressures, reduced access to HCPs and increasing generic competition.

This extremely challenging environment, driven by regulators and market dynamics, increases the potential for employee misconduct - either deliberately (e.g., kickback payments to doctors or 'channel stuffing' through wholesalers/distributors) or through an inability to respond to changing legislation - such as the HCP state reporting initiatives.

What is HCP state reporting?

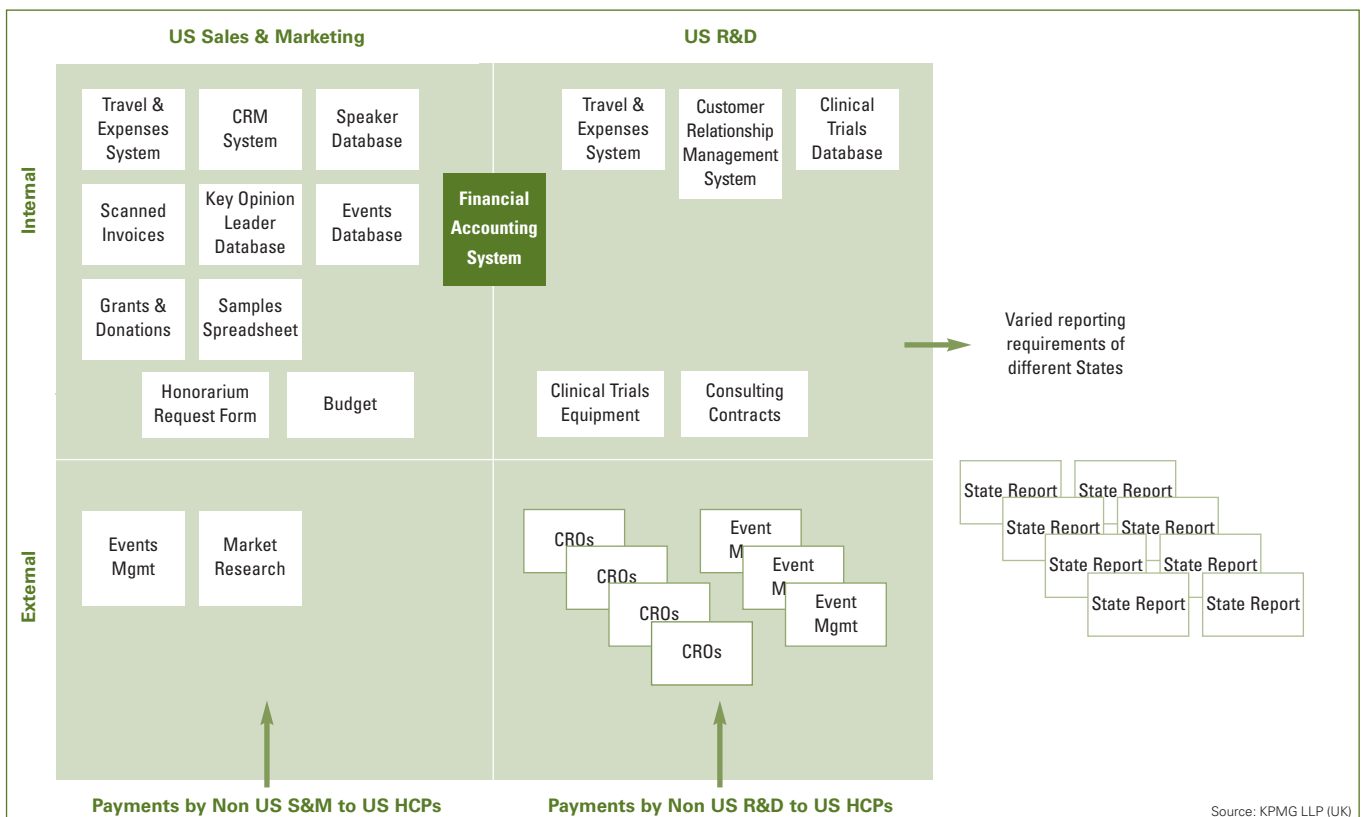
HCP state reporting requires pharmaceutical companies to provide information to a number of US states on the amounts of money spent on individual physicians and institutions including gifts, consulting agreements, meals and travel costs.

Pharmaceutical companies are currently encountering a number of challenges in bringing together the relevant reports including:

1. Ensuring a complete set of data is identified from across the US organisation and from affiliate organisations abroad.
2. Ensuring the accuracy and integrity of data provided by third party agents and suppliers (e.g., event management companies and clinical research organisations).
3. Devising robust business rules for the efficient and consistent processing of data and a justifiable audit trail of decisions.

¹ Source: IMS Health, IMS Integrated Promotional Services, March 2006.

² Source: Kaiser Family Foundation, May 2007.



Source: KPMG LLP (UK)



What are the potential implications of inaccurate reporting?

Failure to disclose accurate information can lead to fines up to \$25,000 per instance. Reputational harm from fines, and the inherent implication that the company has inadequate internal controls in place to understand expenditure decisions, is also likely to impact on shareholder value. Individual executives responsible for reporting and corporate compliance programmes may also come under threat of prosecution if requirements are not met.

Identifying fraud and misconduct

The data set created through this initiative will contain various payment types and activities originally entered by individuals into disparate electronic systems. The unification of this data means that it can be mined by skilled forensic technology professionals to identify potential fraud and misconduct including:

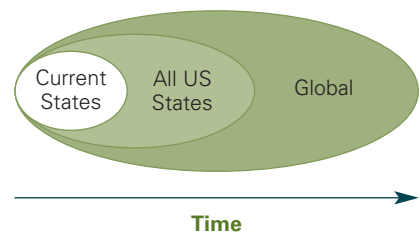
- Breaches of regulatory compliance such as corrupt payments, over-sampling and excessive or improper entertainment.
- Overriding of internal standard operating procedure controls such as sign off and approval processes.
- Duplicate and/or over payments to suppliers and non-compliance with preferred supplier lists.
- Greater insight into activities with HCPs conducted through third parties such as event management companies, clinical research organisations and patient groups.
- Expense fraud by customer-facing teams.
- Tracking of devices loaned to HCPs as part of clinical trials, not collected after completion of the trial, which may be viewed as a form of bribery.
- Donations, sponsorship and cash payments that are inappropriate or way beyond normal or acceptable levels.
- Diversion of budgeted spend to other non-sanctioned parts of an operation.
- Incorrect or false accounting in the books and records to conceal improper activities.

The future

The focus on the integrity of pharmaceutical company expenditure on HCPs is likely to continue. Potential future developments could include:

1. **Extension** of the expenditure types to be reported (e.g., continued professional education, clinical trials and samples).
2. **Geographic expansion** of similar reporting models to all US states and Europe if benefits are seen from the current initiative.
3. **Publication** to the public of expenditure on individual HCPs by each pharmaceutical company.

Potential Roll out of Regulations



Source: KPMG LLP (UK)

“Reputational harm from fines, and the inherent implication that the company has inadequate internal controls in place to understand expenditure decisions, is also likely to impact on shareholder value.”

“The focus on the integrity of pharmaceutical company expenditure on HCPs will continue.”

How should pharmaceutical companies respond to the challenges of HCP state reporting?

Pharmaceutical companies should take a two-pronged approach to addressing the challenges of HCP state reporting:

1. **Respond to the current requirements to report for 2007** – ensuring all business decisions are documented and expenditure allocated accurately to each HCP, according to individual state requirements.

2. **Set the future strategy – and think global.**

It will soon be unacceptable to continue to respond on an ad-hoc basis to each state. Furthermore, expenditure should be allocated to an HCP at the point of data entry, rather than retrospectively at year end. This will require companies to:

- Create a compliance **culture**, educating internal customer-facing teams in the need for accurate customer interaction reporting.
- Update internal **processes** to reflect the state reporting and compliance requirements especially with regard to customer-facing activities and teams.
- Embed processes through **IT systems** requiring certain data to be recorded and alerting users to proximity to payments thresholds.
- **Monitor changes** to state (and national) laws to ensure new legal requirements are incorporated into the reporting structure.
- **Review and report** regularly on activity of customer facing teams.

For non-US affiliates of US organisations there will be a need, in the short-term at least, to provide detailed information on expenditure on US physicians. However, it would be wise to start considering plans for enhancing reporting capabilities, in the event that European governments follow the US lead.

Why should they do this?

Pharmaceutical companies that adopt a proactive approach to HCP state reporting are likely to benefit from identifying at an early stage potential threats of regulatory non-compliance, and more importantly deploying resources efficiently to gain a competitive advantage.

This can include:

1. **Greater assurance** that a robust, accurate and defensible process for data assimilation, analysis and reporting is in place.
2. **Efficiencies and time saving** from not reporting on an ad-hoc basis.
3. **Focus on priority promotional activity** through the ‘capped’ limits on promotional spend meaning costly, non-value-add activity should be curtailed.
4. **Payment restructuring opportunities** with third party providers through greater scrutiny of their work.
5. **Tighter controls** on operational expenses to identify potential fraud and misconduct.
6. **Better customer segmentation and targeting** through holistic view of HCP activity across the organisation.

Which US States are affected by reporting requirements? (As of March 2007)

- California
- District of Columbia
- Maine
- Minnesota
- Vermont
- West Virginia



Simon Tottman
Senior Manager
KPMG Forensic in the UK
simon.tottman@kpmg.co.uk
020 7694 5514



Hitesh Patel
Head of Pharmaceutical and Life Science
KPMG Forensic in the UK
hitesh.patel3@kpmg.co.uk
020 7311 3571

Tracing and Recovering Stolen Funds: The Civil Approach

David Hilton

A variety of options are available to the victims of fraud when attempting to recover their financial loss. David Hilton from the fraud and financial investigations team at KPMG Forensic examines some of the key factors to be taken into account when investigating a fraud and attempting to recover stolen funds or assets through the civil courts.

Fraudsters and other financial criminals have, on many occasions, proven their imagination and intelligence, in the variety of methods used to hide the proceeds of their crimes. It follows that to recover the cash and assets which they have removed and concealed – sometimes with the benefit of careful forethought and planning over months or even years – requires a similar level of inventiveness and creativity, together with a thorough understanding of the legal options available. Below are some of the elements that need to be considered when investigating and attempting to recover cash and assets.

Initial response

The initial response to a suspected or actual misappropriation of funds should be a swift assessment of the situation. How much has been taken, from where and by whom? This relies on prompt information gathering from the victim and their business complimented by external intelligence on the individuals, institutions and countries involved.

It is vital to establish the scale of the misappropriation as well as the knowledge, skills and capability of the suspected perpetrators. The approach to recovery is likely to be very different in a case of relatively minor employee fraud, as opposed to a case where substantial funds have been transferred by an experienced fraudster with established offshore structures in place to facilitate the movement and concealment of assets.

Other factors such as the time since the transfer of funds, and the international scope of the suspected dissipation, will affect what immediate actions need to be taken.

Knowing how to gather information and potential evidence quickly, within the constraints of relevant legislation such as (in the UK) the Data Protection Act 1998, Regulation of Investigatory Powers Act 2000 and the Human Rights Act 1998, together with an ability to recognise and act quickly upon all leads and clues that arise, can make all the difference in the chances of recovery.

Establishing the facts

It may seem obvious to state but for any recovery to be made it is essential to establish where the assets are, and under whose control. However, although this can sometimes be established quickly and easily, in many cases it requires a thorough investigation incorporating external intelligence and the considered use of search, disclosure and/or freezing injunctions. In these cases maintaining a strategic, step-by-step approach can be vital for a successful outcome.

It is important to establish early on which jurisdictions are involved and which entities need to be targeted as part of the investigation. In cases where funds have been entered into a well-established money laundering system, the question may not be 'where are the funds, and under whose control?', but rather 'where were the funds last and who knows what happened to them next?'

Speed is undeniably of the essence but more important is an informed and targeted response to the facts and individuals identified. Money can be moved in seconds but only with the benefit of knowledge, experience, careful planning, established financial structures and reliable professional advisors (either knowingly or otherwise). Transferring physical assets takes longer but similarly relies on trusted intermediaries. Targeting these individuals or institutions can often be the first stage in locating, restraining and recovering assets.

Use of interim orders

Interlocutory or interim civil orders are powerful tools in the recovery of funds. They can compel disclosure of information, authorise searches, and freeze assets nationally and internationally.

However, their use is tightly controlled and a strong *prima facie* case is needed. Often the accounting and financial evidence underpins the application, and must be presented effectively to make a compelling argument for the order to be made.

It is worth remembering that even after issue, civil orders require constant monitoring and evaluation to ensure the issuing court is kept up-to-date with all material disclosure, the scope of the order is not exceeded, or to refute an application for dismissal.

Obtaining a legal judgment

Obtaining a strong civil or criminal judgment in a jurisdiction which enables overseas registration and enforcement should be high on the agenda of an asset tracing team. This can allow a variety of enforcement actions to follow, including backward tracing of funds from a suspect or defendant's identifiable assets.

Deciding on jurisdiction

In a case where multiple jurisdictions are involved, a number of options exist as to where to apply for legal orders and injunctions. It is often beneficial to approach the most co-operative jurisdiction first in an attempt to obtain disclosure or obtain a sound judgment which can then be registered elsewhere.

For example, transactions in US dollars are subject to the US legal system via the correspondent accounts used to effect the transfers. Applying for an order under section 1782 of the US Code can compel disclosure from individuals or third parties with relevant knowledge of US dollar transactions, even if the respective parties do not reside within US territory. This is often a more expedient route to obtaining disclosure than approaching a potentially unpredictable jurisdiction direct.

“It is vital to establish the scale of the misappropriation as well as the knowledge, skills and capability of the suspected perpetrators.”



Going down the insolvency route

Insolvency law is one of the most powerful pieces of legislation which enables assets to be identified and recovered in the UK. However its use requires careful consideration of the situation, as it can often mean a loss of control for the victim as well as the sharing of any recovered funds with other creditors, some of whom may have preferential claims. It can be particularly useful when dealing with trusts in offshore jurisdictions.

Using a multi-disciplinary investigative team

Close co-operation between law enforcement, accountants and legal representatives is vital to make effective use of individual skills and expertise throughout the investigation. Regular and timely communications, and even co-location of personnel, can enable a rapid and joined-up response to fast-moving events. Regular strategic reviews are also important to ensure the direction and focus of the case is re-evaluated as developments occur.

The fluid and dynamic nature of investigations

As information is discovered and developments arise, the direction and understanding of the investigation can change quickly and dramatically. It is vital that experienced professionals are on hand to assess and react to such events, as well as casting a challenging eye over the results. Unsurprisingly, even when compelled to do so fraudsters often do not tell the truth and information can be (and in our experience often is) inaccurate or misleading, whether intentionally so or not.

Conclusion

There are a host of factors to consider when attempting to trace and recover lost funds. Perhaps the most crucial element is a team of experienced and pragmatic professionals who can help ensure that an effective course of action is taken to improve recoveries in an efficient and cost-effective manner.

Asset tracing investigation in practice

KPMG Forensic in the UK was asked to investigate and subsequently trace the stolen funds misappropriated in one of the largest ever frauds in Europe. In the early 90s a large European conglomerate collapsed after a series of thefts by senior management totalling over US \$450 million (in a single transaction over US \$100 million was transferred to one of the fraudsters' offshore accounts). Over the 15 years since the discovery of the thefts, KPMG's Forensic practice has assisted in the undertaking of asset tracing and recovery actions in the UK, Spain, US, Channel Islands, Switzerland, Cayman Islands and Bahamas, which to date have recovered over US \$230 million. FF23

“Close co-operation between law enforcement, accountants and legal representatives is vital to make effective use of individual skills and expertise throughout the investigation.”



David Hilton

Manager

KPMG Forensic in the UK
(on secondment to KPMG in Greater
China until June 2009)

david.hilton@kpmg.com.cn

+86 (21) 2212 3748

An era of raised expectations

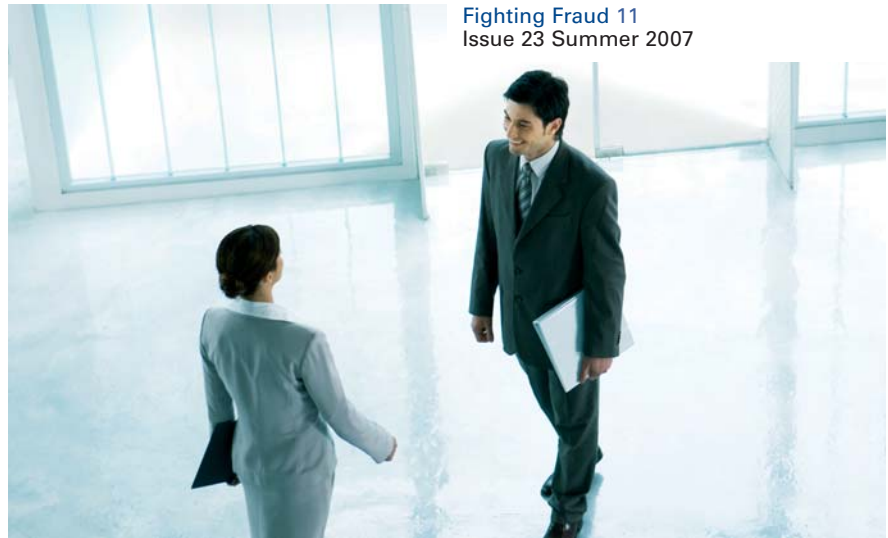
Recent years have seen significantly raised expectations of the role played by financial institutions in preventing and detecting fraud and money laundering. Regulators and prosecutors around the world, armed with increasing powers, are expecting continuing investments to be made to ensure ever more robust systems and controls are put in place.

Fraud, Money Laundering and the Insurance Industry

David Hicks

Jonathan Peake





This reflects a desire by governments to engage financial institutions as partners in the fight against financial crime, as well as a readiness to hold senior management of firms to account when breaches have occurred.

Much of the impact has been felt by the banking sector, which, for obvious reasons, is perceived as the front line against financial crime. The insurance industry has not, however, been immune. This article looks at some of the challenges facing the industry, across both the general and life sectors, and some examples of emerging good practice.

Claimant fraud

Claimant fraud tends to dominate discussion of financial crime in general insurance. This includes both 'hard' fraud such as faked traffic accidents, and exaggerated claims which are known as 'soft' fraud. Market research has largely found the public to have a relaxed view towards the latter, with many people openly admitting to having exaggerated claims on the basis that insurers are considered fair game. This only underscores the scale of the problem.

The old fashioned attitude of the insurance industry that claimant fraud is simply taken on the chin as a cost of doing business is no longer acceptable. In a softening market, the pressure is on, as never before, to combat this widespread crime.

The FSA has made clear that it is engaged on this issue. In the 2006 edition of its Financial Risk Outlook, it reported that claimant fraud continues to be one of the largest fraud categories across the financial sector (over £1 billion for retail lines and £500 million for commercial lines). It is working with industry bodies to find ways to reduce this; in its 2007 edition of the Outlook, the FSA notes a number of positive recent developments within the industry and its trade association, the Association of British Insurers, which has sought to encourage an environment of knowledge sharing, rather than competition, between its members.

One important initiative has been taken by several major general insurers in the UK who are sharing claims data so that this can be mined for linkages and patterns which help identify

organised crime rings. This co-operative approach between insurers has been driven by both public interest as well as a commercial motive for the insurers themselves to look to reduce claimant fraud, and together these drivers are stimulating significant innovation.

The use of increasingly sophisticated data mining techniques is proving effective, and the recently launched Insurance Fraud Bureau has been vocal in advocating the use of advanced data analytics to spot these fraudulent claims, with particular emphasis having been placed on the motor insurance industry. KPMG Forensic has developed sophisticated tools in this field to allow insurers to highlight and detect both organised claims rings and opportunistic frauds within their claims databases.

Other approaches to claimant fraud such as implementing voice recognition systems, permitting a real time analysis of claimants' voices, are also being trialled in several major general insurers with particular emphasis on motor and home insurance claims.

It will be important for the government to support the industry's fight against claimant fraud by ensuring that serial offenders are investigated and prosecuted. There is some scepticism within the industry about the priority that the police attach to tackling financial crime generally, especially given budgetary and resource constraints. Where organised gangs are involved, it is hoped that the Serious Organised Crime Agency, launched in April 2007, and now incorporating the Assets Recovery Agency, will play a role in addressing this perceived deficiency.



“A key point is that senior management must ensure proper and rigorous risk assessments are carried out and that internal money laundering prevention resources are focused on the areas of higher risk.”

Money laundering

Life Assurance business is subject to the Money Laundering regulations and therefore has been impacted by the sustained regulatory focus over recent years. It has long been recognised that life products are prone to attract money launderers because these policies offer ‘living benefits’ such as cash surrender values or income payments. Launderers often either seek to redeem such policies, thereby obtaining a cheque from a clean impeccable source, or else will use the policy as security against a loan. They are prepared to suffer often significant redemption penalties in return for a ‘clean’ cheque from an insurance company.

Although not a regulated business for money laundering purposes, the general insurance industry nevertheless cannot afford to ignore the area as it is still subject to the provisions of UK Proceeds of Crime Act 2002, and general insurance products have been used as part of laundering techniques.

The Guidance Notes issued by the Joint Money Laundering Steering Group, which came into force in September 2006, contain specific guidance for each sector subject to the regulations. This helpfully clarifies expected practice for life companies in combating money launderers. A key point is that senior management must ensure proper and rigorous risk assessments are carried out and that internal money laundering prevention resources are focused on the areas of higher risk. Such risk assessments are expected to be undertaken regularly to ensure new threats are identified and addressed.

In practical terms these assessments have seen Life Assurers undertaking extensive reviews of their customer base to identify individuals classified as Politically Exposed Persons (PEPs)* or those from higher risk jurisdictions. Institutions are then faced with deciding whether any further due diligence is required immediately for these customers and how to implement an enhanced monitoring strategy for those individuals identified in these reviews as higher risk.

This risk-based focus is further reinforced by changes which the FSA has also recently made to its rules. Whilst discarding its detailed money laundering rules, which reflects the reality that many firms look for detailed guidance to the JMLSG guidance notes, it now places great emphasis on the responsibility of senior management to maintain effective AML controls using a fully risk-based approach.

Life companies, as with other firms subject to the Money Laundering Regulations, should now be assessing their compliance with the new rules, as well as the sector guidance issued by the JMLSG, and many already have projects underway to do this.

The sales network

Increasingly life companies sell products not through their direct sales force, but through IFAs, often companies or individuals with little accountability to the insurer. Collecting customer information typically falls within the remit of such IFAs, and this includes obtaining all the Know Your Customer (KYC) documentation required for anti-money laundering purposes. Crucially, although the insurer may require the IFA to gather KYC documentation, in the regulator’s eyes the responsibility lies with the insurer itself.

IFAs present further risks to the insurer, such as ‘churning’, where customers have their policies cancelled by their IFA and are then placed into a new contract, often in the same product, thereby allowing the IFA to receive a commission fee twice for one customer.


The risks insurers face in their distribution channel, through IFAs and other devolved sales staff, can be exacerbated when such individuals are based in differing jurisdictions from the insurer. In order to address the risks posed by IFAs, companies must be proactive in reviewing both the information provided by IFAs and the IFAs themselves. Many firms perform regular audits of their distribution channel, performing on-site visits to IFAs. Additionally, some firms are beginning to profile their sales network through data mining (as discussed above) to spot unusual and suspicious trends within particular networks.

* PEPs will typically be individuals of potentially higher risk, such as diplomats or politicians.

A joined-up approach needed

This article has touched on only a small number of issues faced by the insurance industry in the area of financial crime. There are many other challenges, including addressing the risks highlighted by the Spitzer investigations in the US (such as the risk of collusion between broker and insurer, and the inappropriate use of financial reinsurance), the avoidance of product mis-selling through proper implementation of TCF (Treating Customers Fairly) initiatives, as well as prevention of frauds, such as procurement fraud, which are not unique to the insurance industry.

In the authors' view the approach advocated in the latest JMLSG guidance notes, which is centred on a regular risk assessment process and the application of often scarce internal resources to the areas of greatest threat, has application beyond money laundering.

A joined-up approach is needed in addressing all areas of risk which are critical to a firm's reputation for integrity. This will help ensure that leading practices are rolled out across the organisation and that the corporate radar screen is as sensitive as possible to emerging threats. Designing and implementing counter-fraud and anti-money laundering arrangements, managing internal conflicts of interest, the avoidance of mis-selling scandals, all need to be addressed in a holistic way. This should be done within an appropriate governance framework, with senior management fully engaged. 

“A joined-up approach is needed in addressing all areas of risk which are critical to a firm's reputation for integrity.”

David Hicks is lead partner for KPMG Forensic's services to the insurance industry. He has assisted insurance firms on financial crime and anti-money laundering reviews, as well as conducting investigation and litigation support assignments in the sector.



David Hicks
Partner
KPMG Forensic in the UK
david.hicks@kpmg.co.uk
020 7694 2915

Jonathan Peake has also assisted a number of insurers on financial crime and anti-money laundering reviews, including a recent three month secondment to a major UK life company to assist the development of its internal fraud prevention team.



Jonathan Peake
Manager
KPMG Forensic in the UK
jonathan.peake@kpmg.co.uk
0117 905 4680

A Practising Manager's Primer on Handling Fraud Investigations

Arvind Chopra

“What do you do when it is one of us?”

Frauds are not normal business. They shock you. They shock you because often they are perpetrated by someone you know. Someone you even meet socially probably. Someone you thought shared the same values. Somebody who was one of us.

External resources have their use!

Response to frauds can vary – A 2004 Fraud Survey conducted by KPMG in Australia and New Zealand showed the following pattern* (See table 1 overleaf).

However at times, the shock of fraud committed by someone trusted paralyses many organisations to indecision. It is at these times when an external consultant is most helpful in my view. If organisations can take away the debate around whether to use external resources or not by having a fraud response plan which mandates consulting with an experienced fraud investigator, it helps

immensely. This leads to another question, what is the timing for such involvement. Normally, in my experience, when there is suspicion of a fraud the Head of Internal Audit and General Counsel besides any relevant Operating Managers are consulted in the process to arrive at the next steps. It is at this stage that having the external consultant helps most. Bringing all these people together allows multiple points of view to be examined. Having external legal counsels is also a good idea. It has to be remembered that each of the parties here will approach the issue from a different angle. While the organisation's internal people will be examining different points of view and be somewhat indecisive; the external fraud examiners will have a more aggressive point of view to go after the errant employees. The external counsels can in such situation however prevail upon what looks best from the organisations point of view.

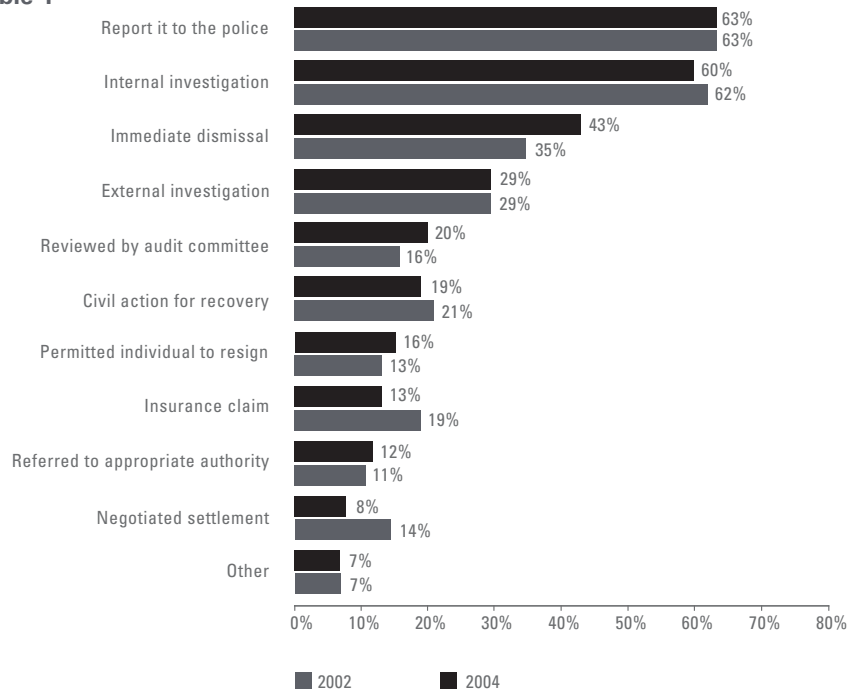
Sometimes the solution of employee dismissal without going through the pains of an investigation may work better.

Keep fact finding focused and closely monitored

The next stage of carrying out the investigation is fact finding or evidence gathering and is the most difficult part of the process. This is where the external fraud examiner is usually best suited to be in the driver's seat. Many organisations may believe that it is best that investigations are led by internal resources. But in my experience, this does not work too well given that many times internal resources are either not experienced enough and have pressures, pushes and pulls from others in the organisation who think they have a better idea of the whole affair. But a word of caution here, if an external consultant or fraud examiner is used they need to be supervised closely.

* Source: Fraud Survey 2004, KPMG in Australia.

Table 1



Source: Fraud Survey 2004, KPMG in Australia

An investigation is a disruptive process; it affects people emotionally at a time when they may already be shocked. It could be a colleague, supervisor, subordinate, friend who is the subject of the investigation. Often if they are also interviewed for facts as part of the investigation, they begin to believe they are also under suspicion. If left unchecked, a large scale round of interviews will leave a lot of people emotionally bruised. It is precisely for this purpose that the progress of an investigation needs to be monitored closely by a sufficient senior manager from the organisation. This will also ensure that culture, language, scope and legal issues are kept in focus.

Report objectively to get results

Having been through the fact finding and evidence gathering the next stage is analysing and reporting. Here the external forensic examiner is of great use because of their ability to present unpleasant facts. And frauds being unpleasant are best reported by people who deal with them regularly. It enables them to deal with these clinically and in a detached way. Here too, it is good to have legal advice on what is acceptable from a privacy protection angle within the country of investigation. Also from the number of investigations I have been involved in, connecting facts and

analysing them meaningfully to report them requires a degree of expertise which is not generally available internally in most organisations. Here too, however, a good review of the facts and tone of the report by a senior manager is a good idea as what works from an organisation culture point of view is very important. Reports can give facts and actions without hurting sensibilities or raising hackles, all of which detract from the issue of dealing with the fraud.

Act to close the chapter

The final stage is acting on the report or results of the investigation. This is best dealt either jointly or without the consultant. The situation may change if there is a decision to pursue criminal action. In such a case the external fraud examiners will have clear guidelines and rules on what they can and cannot do.

They need to preserve their independence if they are to appear as a witness. But generally, many frauds do not result in such a pursuit as organisations prefer to deal with dismissing errant employees rather than criminal actions. However, on how to deal with the employee and how to communicate with them is best done jointly with a lawyer and the external consultant.

Dos and don'ts

Summarising through the various stages of the fraud investigation process elaborated above I would suggest the following dos and don'ts.

Fraud response policy – do have a fraud response policy in place - it cuts the debate on what to do next.

External consultant – do have an external fraud examiner involved - it brings an expert dispassionate point of view.

Lawyers – do have both external and internal legal counsels involved - it gives you more options.

Keep it focused – do not let the external fraud examiner left unsupervised - the disruption can be immense.

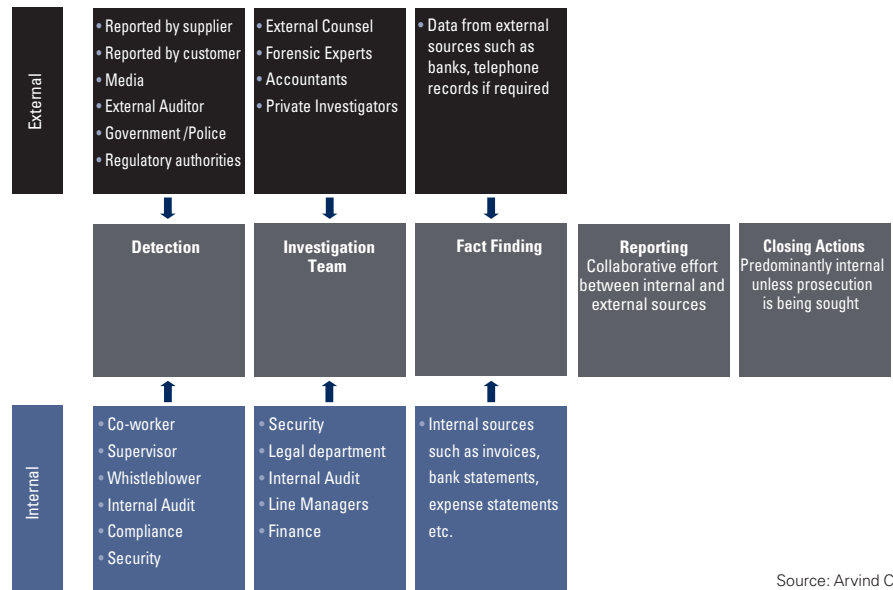
Senior internal resource – do have some senior managers and heads of internal audit fully involved - it will keep the investigation focused and organisational culture and issues taken care of.

Reporting – do have the external consultant take the lead in reporting - it takes away the subjectivity.

Communication with the fraud perpetrator – do have both external fraud examiner and legal counsels involved in communication - it will ensure you are prepared from any angle.

Prepare for the next one – do have the external consultant prepare a fraud response policy, it will help you to be prepared for the next fraud. Chances are if it happened once... it will happen again.

Fraud Investigation Process – A Schematic



Source: Arvind Chopra

Closing words

Frauds are unpleasant but they have their uses. Here is a story I want to leave you with. After years of trying to explain to my seven-year-old daughter what an accountant (which I am) is, I only left her unimpressed. I tried – “a person who is good at maths,” “Can figure out how companies make money” – but none of these cut any ice. Finally on my way to investigate a reported fraud, I tried a new one - “Daddy’s a detective who finds money which people steal from their company”. There was a definite gleam in her eye, I thought. After a bit I went along to her school and did I get a lot of admiring looks from her class. Frauds may be unpleasant but we have to live with them and what else could make Dad a hero and put a strut in his walk. FF23

“The shock of fraud committed by someone trusted paralyses many organisations to indecision.”



Arvind Chopra
Former Chief Compliance Officer
Mittal Steel Company N.V.

White Collar Crime: The Electronic Avenue

Paul Tombleson
Georgina Lewis

The storage capacity of modern electronic equipment provides investigators with the ideal starting place in their search for evidence. Paul Tombleson and Georgina Lewis from KPMG Forensic report.



“The routine destruction or recycling of back-up and other electronic media may need to be halted.”

Anyone investigating wrongdoing may be faced with a mass of potentially relevant information stored on electronic media. The trick for the lawyer is being able to navigate that maze quickly and focus on the key information. Technology creates problems, but it also creates solutions. Technology is available to collect data from electronic media and process it down to a manageable amount for review. Concept-mapping technologies now available in the UK can further reduce the investigator's burden and speed up the review.

The importance of electronic evidence

Electronic evidence is important for a number of reasons:

There is a large amount of it.

It is durable - 'delete' on a computer does not mean 'delete', so it is possible for specialists to retrieve such data.

It includes new types of objective documentary evidence - computers routinely store 'invisible' information without the knowledge of the user (metadata), for instance as to when a particular letter was created, modified or read, and by whom and when.

The casual nature of e-mails makes them a rich source for revealing evidence.

So what strategies exist to allow investigators to attack the mountain of electronic evidence in a methodical way?

The first stage is to plan the collection and review of electronic evidence carefully, prioritising different sources or types of evidence. Will the electronic evidence be reviewed using an electronic document management system or another type? The review strategy may impact on the strategy for prioritising the collection of data.

The next step is usually to secure the data. The routine destruction or recycling of back-up and other electronic media may need to be halted. It may also be sensible to take an immediate back-up as a snapshot of the data at that time.

Investigators need to identify the individuals who may have created or received relevant electronic data and then locate it. There are typical forms of media/data to consider.

- **Laptop and desktop computer hard drives**
- **Shared areas on network servers;** e-mail files are usually stored on a dedicated e-mail server, while documents relating to a specific project may be stored in a folder on a dedicated drive.
- **Portable media;** when collecting electronic media, take a walk around and ask questions. Individuals often have idiosyncratic ways of storing data and it is better to find 30 CDs in someone's bottom drawer at the outset rather than four days before trial.
- **Back-up tapes**

- **Live databases** (e.g., stock, sales, accounting and client relationship management databases) tend to be 'living' documents that evolve each day.

In relation to each of these forms of media, a strategy should be formalised for collecting the data. It is possible to take a forensic image of many of these media. This involves taking a bit-by-bit replica to standards that are acceptable in a criminal court. This is often the best way to deal with hard drives on laptops and desktops. It may not be possible, proportionate or cost-effective to image other media. In some cases, it might be more sensible for the IT director to extract copies of relevant mailboxes and shared folders from servers. Similarly, you may decide to take a 'snapshot' of any live databases at a particular point in time.

Before the data collected can be provided to the investigators for review (whether on an electronic or other document management system), it will need to be processed to remove irrelevant and duplicate or near duplicate material (particularly in e-mail chains). Computers routinely contain masses of data of no interest to investigators, such as operating system files. Typically, the process of relevance filtering is conducted by focusing on particular file types, particular date ranges or particular keywords relevant to the issues. The particular keywords will vary depending on the facts of the case and it is important to agree on these at the planning stage. But keyword



searching can be less effective at reducing the data set to a manageable level in investigations than when used in disputes. In a dispute, the issues tend to have crystallised already. In contrast, investigators often want broad search parameters as the issues have not yet crystallised fully.

Once the data has been filtered for relevance, the remaining data set may still be too large for a cost-effective review of every document. Other tools may be required to focus on relevant material quickly. It is anticipated that there will be an increasing reliance on concept mapping applications, such as *Attenex*[™] and *Autonomy*[™]. Essentially, these work by searching the content of the documents automatically for the nouns or concepts used.

With a combination of understanding the language used and statistical connections, the application detects nouns or concepts that are connected. The application then represents the entire data set visually in a diagrammatic form, connecting clusters of documents on similar issues. Thus the data 'speaks' for itself, enabling efficient review by issue. As the investigator gains leads in an inquiry, it is possible to recluster the documents around, and focus on, identified issues of specific interest. These applications are therefore flexible enough to meet the developing demands of an investigation. These applications can also be used to show social network maps, to identify in diagrammatic form the individuals that have been corresponding with each other and on what issues.

Such applications can be particularly effective at identifying quickly hot spots of activity that might otherwise take a long time to expose by conventional investigative methods.

For instance, in one case the use of the *Attenex* application exposed a large number of documents using baseball terminology, such as 'reaching first base' and 'hitting a home run'. In fact, these were code words used to indicate the fact and extent of the payment of secret commissions. Concept maps are therefore a useful tool to expose the secret code employed by wrongdoers.

As these applications have the power to process and categorise automatically thousands of documents very swiftly, they are powerful weapons in an investigator's armoury. Indeed, it is possible to deal in a similar way with paper records, audio files or even audio-visual files. Some businesses are already routinely storing telephone conversations for several years on back-up tapes. It may not be long before this extends to recordings of voicemails and video conferences. To date of publication, the only viable approach in such cases has been to employ an army of human resource to listen to the audio files. Concept-mapping engines, then, are likely to represent the future of investigations. FF23



Paul Tombleson
Head of Forensic Technology
KPMG Forensic in the UK
paul.tombleson@kpmg.co.uk
020 7311 3964



Georgina Lewis
Director
KPMG Forensic in the UK
georgina.lewis@kpmg.co.uk
020 7694 5133

This article first appeared in *The Lawyer*, 12 June 2006.

KPMG in the UK

Adam Bates
Tel +44 (0) 20 7311 3934

Karen Briggs
Tel +44 (0) 20 7311 3853

Jeremy Outen
Tel +44 (0) 20 7311 3861

Alex Plavsic
Tel +44 (0) 20 7311 3862

Richard Powell
Tel +44 (0) 161 246 4044

Paul Tombleson
Tel +44 (0) 20 7311 3964

KPMG in Argentina

Geronimo Timerman
Tel +54 11 4316 5980

KPMG in Australia

David van Homrigh
Tel +61 (7) 3233 3205

KPMG in Austria

Gert Weidinger
Tel +43 732 6938 2107

KPMG in Belgium

Els Hostyn
Tel +32 (0) 2708 4362

KPMG in Brazil

Werner Scharrer
Tel +55 11 3245 8318

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 China and Hong Kong SAR

Mark Bowra
Tel +86 21 6288 3053

KPMG in Denmark

Torben Lange
Tel +45 3818 3184

KPMG in France

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

KPMG in Germany

Dieter John
Tel +49 221 2073 1575

KPMG in India

Deepankar Sanwalka
Tel +91 124 3074302

KPMG in Ireland

Andrew Brown
Tel +353 410 1147

KPMG in Italy

Gabriella Chersicla
Tel +39 02 6763 2440

KPMG in Japan

Mahito Ogawa
Tel +81 3 5218 6770

KPMG in Korea

Mark Leishman
Tel +82 (2) 2112 0882

KPMG in Luxembourg

Eric Collard
Tel +352 22 51 51 7240

KPMG in Malaysia

Woonchee Ooi
Tel +60 (3) 2095 3388

KPMG in Mexico

Shelley Hayes
Tel +52 55524 68300

KPMG firms in the Middle East

Colin Lobo**
Tel +971 (6) 517 0724

KPMG in the Netherlands

Rens Rozekrans
Tel +31 20 656 7781

KPMG firms Offshore Financial Centres

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

KPMG in Russia & CIS

Ian Colebourne
Tel +7 495 937 2524

KPMG in Singapore

Bob Yap
Tel +65 62132677

KPMG in South Africa

Petrus Marais
Tel +27 (21) 4087 022

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).

© 2007 KPMG LLP, a UK limited liability partnership and a member firm of the KPMG network of independent member firms affiliated with KPMG International, a Swiss cooperative. All rights reserved.

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

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

Publication name: Fighting Fraud 23

Publication number: 307-380

Publication date: July 2007