



Quick Links:

## Cutting through the smoke and mirrors Forensic Focus



**It is great to take time out every now and then and focus on achievements.**

Bernard Madoff's \$US50 billion ponzi scheme in the United States and the \$1 billion Satyam fraud in India have generated considerable headlines over the last few months. In this newsletter we describe how managers commit financial statement fraud and indicators that may help you identify it occurring.

Interviewing people is, often an unrealised, integral part of many peoples jobs. Our team attended a one-day in-house interview training session lead by Don Rabon, a leading instructor of interviewing techniques. Some of our staff also attended a further two-day session led by Don that was open to the public. Don is from the United States and has trained US Secret Service, FBI, NATO, US Army, the CIA and a number of other law enforcement and security agencies. The training session was focussed on detecting deception, which is a critical skill when interviewing suspects and others in investigations. We highlight some key points that you can apply to your interviews.

We are delighted to become the first private sector provider in New Zealand to obtain Encase Enterprise, enabling our forensic team to review electronic evidence on multiple computers at once. Jon Pearce spent two weeks in Sydney, completing training and

accreditation as part of this process. We feature the benefits of completing computer forensic activities at an enterprise or network level in this newsletter.

Deloitte's Forensics team in New Zealand and Australia recently took part in the Knowledge Discovery and Data Mining Cup 2009, an event described as the "Analytics Olympics". The KDD Cup required analytics teams from industry and academia around the world to develop the most accurate model for predicting future events, such as a customer taking their business to a competitor. We highlight the KDD Cup and the commercial value in being able to apply this predictive modelling technology for improving your credit scoring, collections, human resources, operations, fraud, etc.

I hope you enjoy the read

Kind regards,

Barry Jordan and team



# Obtaining the truth the whole truth and nothing but the truth

## Quick Links:

**Obtaining the truth, or at least detecting if someone is being deceitful, is an art form that we could all use everyday. It is a skill that we would like to think we have, but very few of us have mastered.**

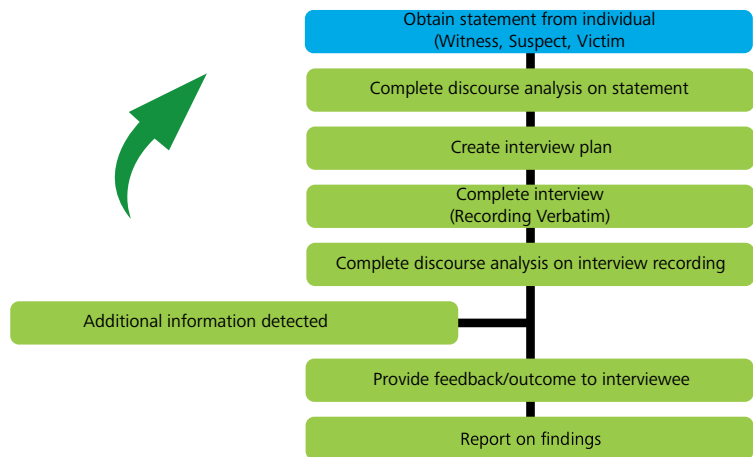
An exception to this is Don Rabon. Don is a professional trainer, specialising in investigative and interviewing techniques, evaluation of depositions, narratives and other forms of discourse. He has trained professionals throughout the world including individuals from the FBI, CIA and US Department of Justice. Recently, we were fortunate enough to attend an intensive training session with Don to sharpen our skills and learn new techniques.

Some key points that we can all apply to interviews are:

- Prepare for an interview where possible and take your time. Make sure you obtain all available information. Given that you don't have the benefits of a first interview again, getting it right first time is vital;

- Be nice to the individual. Playing 'bad cop' will fail more times than it will work;
- Work on the 'innocent until proven guilty' mentality. If you use this approach you will have a more stable and objective argument when providing your findings;
- Record the interview where possible. This will provide you with the ability to continuously analyse what was said and protect all parties from accusations of inappropriate behaviour;
- Never presume what the person means. A deceitful person will often be vague about what they are telling you so it's important to confirm what they are saying rather than presume you understand.

The above points assist with what approach to take, but there is also a process you can follow to help you achieve full value from your interview. The following summarises what Don suggested:



So, next time you are trying to obtain information from someone who may be reluctant to provide the details you are after, consider the tips and techniques set out above. Or, if you want to obtain more information on interviewing and detecting deception, contact Lorinda Kelly.



**Lorinda Kelly**  
+64 (0) 4 474 7859  
[lorkelly@deloitte.co.nz](mailto:lorkelly@deloitte.co.nz)



# Financial Statement fraud

## What are the signs?

### Quick Links:

**Bernard Madoff's \$US50 billion ponzi scheme in the United States and the \$1 billion Satyam fraud in India are two high profile examples of financial statement fraud. It seems likely New Zealand has not been immune from this, with many finance companies reporting high levels of profit and strong balance sheets, only to be placed into receivership months later.**

Investors, lenders, creditors, shareholders and insurers are all vulnerable to financial loss caused by financial statement fraud.

There are often signs that financial statement fraud is occurring, if the fraud is significant. Harry Markopolos, a US based Certified Fraud Examiner, had a hunch that Mr Madoff was running a ponzi scheme because he found it difficult to believe that Madoff could generate such consistent returns for investors over a long period of time. He modelled Madoff's investments and determined that the returns were mathematically impossible to achieve. Mr Markopolos first took his concerns to the Securities and Exchange Committee ("SEC") in 2000. He resubmitted evidence to the SEC in 2001, 2005, 2007 and 2008, but the authorities took no action.

Although some financial statement frauds occur where unscrupulous executives actively create assets that never existed (e.g. reporting non-existent bank balances), many financial statement frauds are

considerably more subtle, often occurring as a result of inactivity. Profits and the financial position of companies can be easily manipulated by managers failing to:

- Write-off or provision for uncollectable accounts receivable and loans;
- Write-off inventory that has reduced in value;
- Accrue for expenses incurred but not paid.

There is often considerable incentive for managers of companies to misstate the financial performance and position of companies to:

- Meet performance targets;
- Maintain employment, salary and status;
- Achieve bonuses;
- Prevent banking covenants from being breached.

As a lender, creditor, insurer, investor and shareholder there are a number of triggers that could allude to statement fraud and you should be asking questions around this possibility when you identify one or more of the following:

- The company is reporting profits, but has tight cash flows;
- Gross profit levels remain at high levels, even though the company is facing pricing pressure in the market;
- Accounts receivable, accounts payable and stock levels are increasing, when sales are flat or declining;
- The company is close to breaching banking covenants;
- There is a significant level of "year-end" adjustments;
- There are significant bonuses available to senior management; and perhaps most importantly
- It doesn't "feel right".

For information on this subject and what to do if you suspect statement fraud please contact Jason Weir.



**Jason Weir**

+64 (0) 9 303 0966

[jasweir@deloitte.co.nz](mailto:jasweir@deloitte.co.nz)

# Advanced Forensic Technology

## The next generation of computer forensics.

### Quick Links:

**Forensic technology is becoming more and more advanced - tools are now available that can deal with computers connected to corporate networks rather than the traditional stand-alone and portable computers synonymous with traditional forensic technology. This progression in technology has greatly enhanced the approach to computer forensics. Here's how:**

#### **Electronic Discovery :**

We were asked by a client to assist them with their discovery process, the twist being that it needed to be done in a very tight timeframe. To meet this goal we used the latest forensic technology software to identify the files that were required for the discovery process. This was done over the company network and did not cause any noticeable downgrading of performance for users, nor prevent normal back-ups to be made. The identified files were copied to a forensic standard and produced for relevance review and disclosure. By doing it this way, the amount of material required for relevance review was reduced from tens of thousands of files down to just a few thousand. This technique meant our client met their rigorous deadline, which would not have been achieved using traditional methods.

#### **Technology has also enhanced intellectual property reviews:**

The ability to use forensic analysis techniques on company networks helps us efficiently locate intellectual property that might have been copied by a member of staff. This made a recent assignment a whole lot easier. We were asked to review a server and several PCs linked to it, looking for evidence their client database had been copied by a former employee. We took a forensic copy of all the material on their server during working hours, without users being notified or any drop-off in network performance. Previously it would have been necessary to shut down the server to take the copy, consequently causing considerable disruption to the business. But because we were doing this in 'real-time', we also were able to review as we copied. Within one hour we were able to demonstrate that a user had extracted commercially sensitive data from the client's system.

#### **Another area is risk reviews:**

It is common for companies to provide more and more computing power to their staff through access to email and the Internet, which can be used to view and distribute inappropriate or illegal material. This material is inevitably being stored on company IT systems. In addition, there is the increased possibility of reputational risk should such material be discovered. We had a client who was concerned that inappropriate material was being saved onto the main server in an area accessible by multiple staff. We connected to the relevant server and previewed what was happening. The material in question was quickly identified and located, and included a large amount of deleted files. As part of our preview, we were able to see which user had saved the files into the common areas. We made a forensic copy of the identified user's computer and provided a report to the client on our findings. The client was then able to act, putting a stop to the unwanted behaviour.

#### **The other area that the enhanced forensic technology tools helps is in a fraud investigation:**

When fraud is being investigated it's not always apparent where relevant material might be located. In the past, investigators have had to manually review electronic material looking for potential evidence on servers. With the introduction of advanced forensic technology software, it is now possible to search live servers and individual computers for electronic material that might assist an investigation. Clients are benefiting from this process as it is quicker, more sophisticated and causes less disruption to their daily business.

For more information on this topic, please contact:



**Barry Foster**

Tel: +64 (0) 9 3030974

Email:

bfoster@deloitte.co.nz



**Jon Pearce**

Tel: +64 (0) 9 3030838

Email:

jpearce@deloitte.co.nz

# The “Analytics Olympics”



## Quick Links:

[Based on what 50,000 customers did with a mobile phone company – can you predict the actions of another 50,000 customers?](#)

Will they switch to another provider, buy another product, upgrade or do nothing at all? That was the challenge in the KDD Cup for 2009. KDD (Knowledge Discovery and Data Mining) is a special interest group of ACM (Association for Computing Machinery), and is one of the premier international forums in the field of data mining and predictive analytics. For the last 13 years KDD has run a contest where the challenge is to be the most accurate predictor of an outcome. This year a Deloitte team with staff from the Auckland and Sydney offices entered against teams from industry and academia around the world.

### The Challenge

The challenge data set was supplied by French telecommunications company, Orange. Having started out as Orange’s real data on customer history and usage, it was heavily disguised before being made public for the contest: text values were encrypted and variable names disguised. This effectively removed a significant element of what we might normally do in a modelling engagement: exploring, augmenting and profiling the data from a business perspective. We were also fortunate to have the data structured as it was, as another big piece of work in a typical modelling assignment is getting the data into the right shape. Instead, the contest became one of minds, methods and machinery – how accurate a team could be in the time available.

We apply a number of tools to a problem such as this, depending on the data and the nature of the problem. In this case the number of records was no issue (having 50,000 customer records to analyse is these days a modestly sized problem) however the number of variables was 15,000, which is considerable but not unrealistic. A number of tools quite simply cannot cope with this much data, however one tool in the bag (The SAS System) was able to readily handle this data with no complaint, enabling us to get stuck into the prediction problem.

### Modelling Process

Those 50,000 customer records tell what customers did in the past. The 15,000 variables contained all the information known about those customers – such as who they are and where they live, what products they have, the services they subscribe to, call usage, unused call minutes and so on. In addition there are flags to indicate a subsequent outcome: whether they have churned, bought or upgraded.

From that history, we want to be able to predict the future – what is the likely outcome for some different customer records. To a company such as Orange this

is vital knowledge. For example, if they know who is likely to switch to a rival company (known as churn), they can take preventative action such as a customer care call or offer a free add-on. The cost of this might be uneconomic to offer to the entire customer base, so a predictive model can be useful to identify those customers most at risk. In this contest Orange provided a second data set of another 50,000 customer records where the outcome is only known to them, not us.

When we make a predictive model we use a modelling tool to identify the relationships between variables and the relative importance of those variables. Usually more than one tool will be used – they each have their strengths and weakness -- but the real test is how well they predict the result. Having created a model we score the second data set customer by customer – essentially making our prediction of what that customer would do based on their data and our model. This scored set becomes the basis for comparing how accurate the competing teams are, and the overall score for the contest is how accurate those scored sets are.

### Results

The competition has just closed and based on overall scores we managed to get in to the top 10% of the worldwide field of industry practitioners and academics. We’ve enjoyed sharpening up our skills on this reasonably meaty analysis.

However what is compelling for me is just how accurate a modelling prediction can be. Despite using disguised data, these predictive modelling techniques can be astoundingly accurate. Being able to predict those customers that are going to leave with 73% accuracy, who’s going to become a customer with 84% accuracy, and who’s going to be “up-sold” and buy another product with 89% accuracy have to be compelling propositions indeed for any marketer.

### Applications

This contest was a marketing application and gave us very real practice in ways to increase our prediction accuracy. However the techniques apply to any situation where there is historical data and an outcome to predict. Examples include credit scoring, collections, human resources, operations, fraud and so on. Key factors to consider in deciding whether predictive modelling might solve a business problem are:

**Economics:** Is there a pressing need to resolve this problem – is it costing money or is there money to be made?

**Data:** Is there sufficient data available or able to be acquired, and is it relevant to the problem at hand?

**Actionable:** Are the insights from the model able to be acted upon? Is it able to be used to influence an outcome?

We hope you enjoyed the read.

We're always keen to hear your feedback, if you have any suggestions for content or topics you would like us to explore in the newsletter please email us on [lisalee@deloitte.co.nz](mailto:lisalee@deloitte.co.nz) >

# Contacts

## Your Forensics and Recovery team:

### Forensics

**Barry Jordan - Partner**

+64 (0) 4 470 3760

[bjordan@deloitte.co.nz](mailto:bjordan@deloitte.co.nz)

**Jason Weir - Associate Director**

+64 (0) 9 303 0966

[jasweir@deloitte.co.nz](mailto:jasweir@deloitte.co.nz)

**Barry Foster - Associate Director**

+64 (0) 9 303 0974

[bfoster@deloitte.co.nz](mailto:bfoster@deloitte.co.nz)

**Lorinda Kelly - Associate Director**

+64 (0) 4 470 3749

[lorkelly@deloitte.co.nz](mailto:lorkelly@deloitte.co.nz)

### Recovery

**David Vance - Partner**

+64 (0) 4 470 3768

[dvance@deloitte.co.nz](mailto:dvance@deloitte.co.nz)

**Rod Pardington - Partner**

+64 (0) 9 303 0705

[rpardington@deloitte.co.nz](mailto:rpardington@deloitte.co.nz)

**David Levin - Partner**

+64 (0) 9 303 0935

[davidlevin@deloitte.co.nz](mailto:davidlevin@deloitte.co.nz)

**Viv Madsen-Ries - Associate Director**

+64 (0) 9 303 0940

[vmadsenries@deloitte.co.nz](mailto:vmadsenries@deloitte.co.nz)

**Garry Clarke - Associate Director**

+64 (0) 9 303 0797

[gaclarke@deloitte.co.nz](mailto:gaclarke@deloitte.co.nz)

## Subscribe or Unsubscribe:

To add other names to the subscription list or have your name removed, please contact Lisa Lee on [lisalee@deloitte.co.nz](mailto:lisalee@deloitte.co.nz) >

## For further information, visit our website at [www.deloitte.co.nz](http://www.deloitte.co.nz)

Deloitte brings together over 900 specialists providing New Zealand's widest range of high quality professional services. We focus on audit, tax, technology and systems, risk management, corporate finance and business advice for growing organisations. Our people are based in Auckland, Hamilton, Wellington, Christchurch and Dunedin, serving clients that range from New Zealand's largest companies to smaller businesses with ambition to grow.

Deloitte provides audit, tax, consulting, and financial advisory services to public and private clients spanning multiple industries. With a globally connected network of member firms in 140 countries, Deloitte brings world class capabilities and deep local expertise to help clients succeed wherever they operate. Deloitte's 150,000 professionals are committed to becoming the standard of excellence.

Deloitte's professionals are unified by a collaborative culture that fosters integrity, outstanding value to markets and clients, commitment to each other, and strength from diversity. They enjoy an environment of continuous learning, challenging experiences, and enriching career opportunities. Deloitte's professionals are dedicated to strengthening corporate responsibility, building public trust, and making a positive impact in their communities.

This publication contains general information only, and none of Deloitte Touche Tohmatsu, its member firms, or its and their affiliates are, by means of this publication, rendering accounting, business, financial, investment, legal, tax, or other professional advice or services. This publication is not a substitute for such professional advice or services, nor should it be used as a basis for any decision or action that may affect your finances or your business. Before making any decision or taking any action that may affect your finances or your business, you should consult a qualified professional adviser.

None of Deloitte Touche Tohmatsu, its member firms, or its and their respective affiliates shall be responsible for any loss whatsoever sustained by any person who relies on this publication.

Deloitte refers to one or more of Deloitte Touche Tohmatsu, a Swiss Verein, and its network of member firms, each of which is a legally separate and independent entity. Please see [www.deloitte.com/nz/about](http://www.deloitte.com/nz/about) for a detailed description of the legal structure of Deloitte Touche Tohmatsu and its Member Firms.