



Quick Links:

## Cutting through the smoke and mirrors Forensic Focus



### Welcome to our final Deloitte Forensics newsletter for 2008!

This has been an exciting and eventful year for us and one in which our Forensic team has grown significantly! Our most recent addition to the team is Andrew Cathie. Andrew will head up our Analytics Insight capability and will be based in the Auckland office. Most recently he has operated as an independent data analytics and business intelligence consultant with clients in New Zealand, Sydney and California. Analytic Insights uses advanced analytical tools to uncover meaningful and useful intelligence from the vast amounts of data that organisations today are amassing. These methods can be applied to diverse applications such as customer segmentation, fraud detection, marketing, credit and operations.

It is hard to believe that our annual Wellington Melbourne Cup function is over for another year and we will soon be heading off for the Christmas break. Whilst the office will be closed from 23 December, and will reopen in the New Year on the 12th of January, if you have the need to contact us over that period, we will still be available by telephone.

In this newsletter we feature the last phase of a fraud investigation – Reporting and Recommendations, “All is fair in love and war” in relationship property disputes, the importance of having your hard drive wiped by an expert and anti-money laundering in New Zealand.

Wishing you and your family a safe and happy Christmas.

Kind regards,  
**Barry Jordan and team.**



# Planning a fraud investigation

## Quick Links:

Forensic accountants perform a variety of investigations. The exact process followed from one investigation to the next will never be the same, however there are themes that remain consistent, like objectivity, impartiality and clear and concise communication.

We have also found that when planning an investigation, there are almost always three phases. These are:

- Phase 1 – Pre-investigation;
- Phase 2 – Investigation;
- Phase 3 – Reporting and recommendations

In previous newsletters we have outlined the first two phases. In this newsletter we will touch on phase 3 – reporting and recommendations. This information should be useful for those who become involved in any kind of investigative process.

### Phase Three – Reporting and recommendations

The pre-investigation planning phase would have identified the potential end users of the report. That phase should also have identified the objectives of the report users. There is no point in conducting an in-depth investigation and reporting upon various breaches of internal control if that is not what the readers of the

The report should also identify ways in which the fraud that has been perpetrated could have been avoided, or can be avoided in the future. Where there have been breakdowns in internal control or a lack of controls these should be highlighted and brought to management's attention.

It is not the role of the fraud investigator to judge a suspected fraudster innocent or guilty. Of course, if a confession has been obtained in an interview that should be communicated to management, however the report should not contain conclusions as to the matter of guilt. The final judgment in this area rests with the Courts, if it is to proceed that far.

The report should also test and report against the proposed hypothesis at the start of the investigation. The report should not be subjective in its conclusions. In our experience, a common failure of many investigators is that having done a book perfect investigation, they "fall in love" with their own work, drawing conclusions that are not supported by the work papers or the evidence. It is essential that before the report is submitted to management in its final form, that the team reviews the report as to its balance, fairness and above all, accuracy.

Assumptions need to be clearly identified as assumptions and equally, subjective statements, need to be identified as such. Conclusions supported by hard evidence and the reference to that evidence should also be identified.

Above all, the report should be clear and decisive in its conclusions avoiding ambiguity and doubt wherever possible. The preferred course of approach where matters are not known is to clearly state that this is so, rather than to hypothesise.

Finally, when the report has been submitted and the job concluded, all work papers and documentary evidence should be secured before being placed into deep storage or destroyed. In our experience, it may take years for a decision to be reached as to whether or not a prosecution will take place.

**For more information please contact Lorinda Kelly.**

---

## A fraud investigator's report should focus upon the key factors establishing how the fraud was committed, who committed the fraud, how much was taken and how reparation may be achieved.

report want. Likewise, if it is not the intention of the recipients of the report to refer criminal charges, writing a report that focuses upon the criminal responsibility of the fraud offender is both ineffectual and a waste of time.

A fraud investigator's report should focus upon the key factors establishing how the fraud was committed, who committed the fraud, how much was taken and how reparation may be achieved.



**Lorinda Kelly**  
+64 (0) 4 470 3749  
[lorkelly@deloitte.co.nz](mailto:lorkelly@deloitte.co.nz)

# All is fair in love and war – relationship property disputes

## Quick Links:

As relationships unceremoniously fall apart, hearts are broken and dreams are shattered, and the amount at stake both emotionally and financially for all parties involved is immense.

Traditionally the role of an accountant in relationship property disputes has focussed on the valuation of assets, particularly businesses.

Increasingly however one party (usually the partner not involved in the business) has concerns that funds have been siphoned out of the business, which in turn understates the total pool of relationship assets in two respects:

- The diverted funds may still be available (e.g. secret bank account);
- The reported profits of the business may be understated, which if undetected will cause the business to be undervalued.

If for example Mr X has diverted \$100,000 p.a. from the business over three years, this may understate the value of the pool of relationship assets by \$800,000, calculated as follows:

Cash in secret bank account	\$300,000
Increased value of the business (additional profit of \$100,000 per annum x discount rate of say 20%)	\$500,000
<b>Total</b>	<b>\$800,000</b>

Clearly there is considerable value for Mrs X in identifying anomalies in the financial reports before the valuations are completed and the relationship property is divided. For this reason many relationship property disputes now require an investigation to be completed before the valuation of the business can be completed.

**For more information please contact Jason Weir.**



**Jason Weir**  
+64 (0) 9 303 0966  
[jasweir@deloitte.co.nz](mailto:jasweir@deloitte.co.nz)



# Data in the wrong hands



## Quick Links:

Most top companies will replace their laptops and computer systems every two to four years based on their computer replacement plan. During the use of these systems, sensitive and confidential data is saved to the hard drive either intentionally or unintentionally. When the new computer systems are rolled out the old computers are usually auctioned off, sold, donated to charities or thrown away.

But what about the sensitive data that is left on the hard drive?

Many people believe the best way to erase information on a hard drive is by formatting it. Contrary to popular belief, formatting your hard drive DOES NOT erase data. The data is still available to anyone who has access to file recovery tools, which these days are freely available on the internet.

In August the Associated Press reported that a computer containing banking security details of more than one million people had been sold on eBay – the latest in a series of losses of personal data in Britain. The computer containing account numbers, passwords, telephone numbers and signatures was sold on eBay without the hard drive being wiped first.

In the wrong hands this sensitive data could be devastating to an organisation or individual. The outcome of such an event could result in identity theft, loss of trade secrets, irreparable damage to one's reputation, civil or criminal liability.

Next time you are thinking of giving, selling or throwing away your old computer ensure the hard drive has been destroyed or wiped by an approved computer forensic expert and preferably, to US Ministry of Defence Standards.

**For more information please contact Jon Pearce.**



**Jon Pearce**  
+64 (0) 9 303 0838  
[jpearse@deloitte.co.nz](mailto:jpearse@deloitte.co.nz)



# Anti money laundering – countering the financing of terrorism

## Quick Links:

Money laundering only became an offence in New Zealand in 1996. Prior to that hiding or attempting to hide illegally gained funds was technically not a crime in New Zealand. Also, providing financial services to a designated terrorist entity only became an offence in New Zealand in 2002, after the Terrorism Suppression Act 2002 came into force. Compounded by a number of international incidents .e.g. '9/11' and the 'London bombings', there has been an increased focus to prevent money laundering and the financing of terrorism.

One of the initiatives that has been set up is the Financial Action Task Force ("FATF"), that includes an international watchdog of which New Zealand is a member country. FATF establishes minimum global standards in relation to preventing money laundering and terrorist financing (more commonly known as the FATF Recommendations). In 2003, FATF reviewed New Zealand's level of compliance with the FATF Recommendations – several areas were found wanting.

The changes recommended by FATF include strengthening the current legislation surrounding identification of individuals, conducting ongoing due diligence and increasing penalties on institutions and individuals for cases for non-compliance. The scope and coverage of the new legislation will be considerably broader than the existing Financial Transactions Reporting Act 1996 and therefore widens the catchment of industries responsible for complying with the legislation.

New Zealand is still 'behind the 8 ball' as far as making the appropriate changes and becoming compliant with FATF Recommendations. It would seem that there is a real 'lets wait and see' attitude surrounding the industries affected. However what we are failing to recognise is that we are lagging behind the rest of the world.

The draft legislation is currently expected to be introduced to Parliament around April 2009 (only weeks before the next scheduled review by FATF), with the legislation passed into law later that year. It will be interesting to see how the industries affected react when these changes to the legislation are finalised.

This is a constantly evolving space and like the rest of the world it certainly wouldn't hurt for New Zealand to start planning and implementing the appropriate changes now.

**For more information please contact Sam Labone.**



**Sam Labone**  
+64 (0) 4 470 3546  
[slabone@deloitte.co.nz](mailto:slabone@deloitte.co.nz)



# Is your identity safe?



## Quick Links:

This year we have seen a dramatic increase in “identity crime” in New Zealand. This illegal activity, largely driven by a desire to make a financial gain, has emerged in two distinct forms: identity fraud and identity theft.

**Identity Fraud** involves the creation of a new, false identity. An example would be the multiple benefit fraudster Wayne Patterson (convicted for defrauding the Ministry of Social Development) who created a suite of 123 fictional identities to claim \$3.4 million in benefit payments over three years.

**Identity Theft** is more common and more pervasive. This is when someone steals the identity of a real person and uses it as if it were their own. A stolen identity is often used by the thief to obtain credit (e.g. personal loans of up to \$10,000) or to buy goods (e.g. second-hand cars, whiteware, electronics). The victim is left to deal with the sense of intrusion, as well as potential liability for the thief’s actions and a damaged credit history.

So far this year, the Deloitte Forensics team has investigated losses in both areas of identity crime, with the amounts involved ranging from \$20,000 to \$1m.

In our experience, we have not seen the *modus operandi* change much: identity theft victims often know the person who uses their identity. The person might be a work colleague, friend, sports club member, teammate or a Facebook/Bebo “friend”.

Fraudsters may go to some lengths to match the victim’s characteristics of gender, age or ethnicity to themselves, in the rare event that an institution calls to check.

There are several steps that can be taken to make it hard for identity thieves – securing and monitoring your own information is very important.

### How can you prevent your identity been stolen?

By taking some simple steps you can make it harder for your identity to be stolen, we suggest:

- take some time to destroy or shred bank statements, credit card bills, letters – especially those from your insurance/bank provider inviting you to accept pre-approved extra cover – invest in a home shredder;
- be cautious about who you give your personal information to (i.e. pet’s name), particularly over the phone – reputable businesses will never ask you for this sort of personal information;
- take steps to protect your computer (firewalls/virus protection), especially if you are a member of online networking sites such as Facebook or Bebo.

### What about your business?

Businesses can also be potential victims. Here are a couple of ideas to secure your staff and your data:

- check the personal data you hold on file about your clients and staff – if you need to retain it, then ensure it is well-protected. Destroy obsolete or old information safely and securely;
- check out the identities of your staff and customers but once you have finished with the information, either return it or safely destroy it;
- if a staff member becomes a victim, getting specialised assistance early will help them – the consequences for individuals may take a financial toll, but the emotional fallout is often more significant.

For more information please contact Barry Jordan.



**Barry Jordan**  
+64 (0) 4 470 3760  
[bjordan@deloitte.co.nz](mailto:bjordan@deloitte.co.nz)



**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)

**Andrew Cathie - Associate Director**

+64 9 (0) 303 0781

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

**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)

**David Levin - Associate Director**

+64 (0) 9 303 0935

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

**Greg Sherriff - Associate Director**

+64 (0) 4 470 3766

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