

**Deloitte.**

# Forensic Focus

*Cutting through the smoke and mirrors*



Welcome to your first Deloitte Forensic newsletter.

As you all know we have now transitioned across to Deloitte and I am happy to report, it has all gone very smoothly and we are now very much business as usual. The reaction to our merger has been overwhelmingly positive – thank you for the many messages of support.

The core of what we do has always been to find innovative ways of solving problems for our clients. One of the real attractions of joining Deloitte is the ability to tap into the global forensic practice. In Australia alone there are 21 partners and over 180 staff in the forensic practice.

We have already established links with our counterparts in Australia and throughout Asia and picked up a few great ideas that we will introduce to the New Zealand market. We have also been able to help out our Australian colleagues by sending a staff member to Australia to assist in a major corruption investigation.

We are delighted to announce the appointment of Sam Labone and Jon Pearse as managers to our forensic team. Sam joins us from ANZ National where he was the fraud manager and Jon joins us from the

Electronic Crime Lab at the Police where he was a computer forensic analyst. The appointment of Sam and Jon increases our core forensic team to nine full-time specialists.

Lorinda Kelly and Barry Foster joined me in presenting a workshop at the inaugural NZ Institute of Chartered Accountants' Forensic Accounting conference earlier this month. We touch on the investigation process we presented later in the newsletter.

We also feature the first wave of litigation from the finance company sector collapse. And, we look at the use of passwords to protect electronic documents, the ability to crack them and our current fertile fraud landscape in New Zealand.

Kind regards,  
**Barry Jordan**



# Investigation

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 that are passed through. These are:

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

In the last newsletter we outlined the first phase, we will now touch on phase two – planning the fieldwork, from a fraud investigation perspective. This information should be useful for those who become involved in any kind of investigative process.

## Phase Two – Investigation

Having completed the pre-investigation planning, the next step is to plan the field work associated with the investigation itself.

The next steps when leading a fraud investigation include:

- Reviewing the internal control system to determine what compliance (or non-compliance) with the system exists.
- Assessing the probable level and extent of complicity within the organisation. (This can be critical to ensure that the forensic accountant does not provide information to, or obtain misleading information from people involved).
- Ensuring the investigation team has the

knowledge, skills and disciplines necessary to carry out the investigation effectively. Qualifications should include professional certifications, such as Certified Fraud Examiner, accounting/legal, reputation, and absence of complicity with those being investigated.

- Designing a procedural methodology that will identify the perpetrators, the extent of the fraud, techniques used, and the causes.
- Coordinating activities with the client and their legal advisors and other specialists, as appropriate, throughout the investigation.
- Being aware of the rights of the alleged perpetrators and personnel within the scope of the investigation and the reputation of the organisation itself.

As the investigation phase is carried out, it is important to regularly review results against the original pre-investigation hypothesis. In particular it is important to keep a focus upon how the fraud was committed and then who could have committed it.

## Evidence

The way documentation that is suspected to be part of the fraud is identified and handled is critical. If in doubt documentation should be secured.

A number of investigators have found to their dismay that computers or documents that may have been used in a fraud were left with the intention of coming back to secure them later, only to find that the documents had been altered or had disappeared altogether.

Once a fraudster is alerted that there is suspicion, it is likely that operations will be shut down and protective measures taken (usually pre-planned for the event) to secure or destroy incriminating documentation.

Finally, if in doubt, the security of documentation and associated evidence should be discussed with legal counsel. Under no circumstances should original documentation be edited or notated by the investigators.

For more information about the investigation process please contact:



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



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

# Finance companies and the wave of litigation

We are now starting to see an upsurge in litigation as a result of finance company collapses. In last month's news headlines we have seen "Bridgecorp Directors Prosecuted", "Investors set to sue financial adviser", "Bankruptcy proceedings start against Petricevic", "Five Star Finance Directors Prosecuted" and "Byers ordered to pay \$13.6m plus interest".

There is a significant number of investigations of loan books and finance companies currently underway, by both public sector enforcement units and private sector investigators. Clearly the volume of litigation in this sector will increase significantly over the next few years.

## Five common themes we have identified from our investigations in this sector include:

- over exposure to a single sector
- focus on quantity rather than quality of lending
- limited focus on the ability of borrowers' to repay loans
- poor and/or fraudulent documentation
- poor loan review and approval processes

While this will be a fascinating area for the next few years for litigators, investigators, insolvency practitioners and "commercial rubbernecks" alike, it is unlikely to provide much comfort for the "mum and dad investors" who have lost their life savings and been provided with a harsh lesson on risk.

## Five warnings signs for lenders, Trustees and advisers:

- Rapid increase in level of funds lent
- Significant and/or increasing levels of defaults
- Unusual clusters of defaults (e.g. many defaulters from same suburb)
- High staff turnover
- Non-adherence to lending guidelines

For more information about this topic please contact:



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



# Password recovery

Good security practices dictate the use of password protection on sensitive and confidential documentation that requires protection. There have been a number of recent instances of confidential information being “found” in places it really should not have been left (like trains, taxis and buses).

What happens when the password for these documents is lost, forgotten or the person controlling the password and subsequently the protected information leaves the company?

Password Recovery is the process of recovering passwords from data that has been stored in or transmitted by a computer system. A common approach is to repeatedly try guessing the password. This can be time consuming and often has little success.

The purpose of password recovery might be to help a user recover a forgotten password, to gain access to a system or file, or as a preventive measure by system administrators to check for easily crackable passwords.

Our password recovery capability enables password recovery from more than 80 applications (including Microsoft Office products).

We harness the processing power of a dedicated forensic network to decrypt files and perform robust password recovery. Using this distributed processing system we can process in excess of 500,000 passwords per second. The password on a Microsoft Office file (word or excel) will normally be recovered within a day.

If you have any questions or need us to assist with your password recovery needs contact:



**Barry Foster**  
+64 (0) 9 303 0974  
[bfoster@deloitte.co.nz](mailto:bfoster@deloitte.co.nz)



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



# Our fertile fraud landscape

The Introduction of electronic financial systems and the internet has undoubtedly changed the where and how we look for evidence to detect fraud but my view is, it is just as complex as 20 years ago.

## So if the complexity is comparable, then what has changed?

- Electronic v Paper – Fraudsters no longer rely on hard copy documents. Cash is now elicited electronically by manipulating internal records and bank accounts.
- Anonymity – Most frauds we investigate are now carried out remotely by staff or customers using log-on access as “verification” of identity.
- Speed – Today it takes merely minutes to execute a fraud. False emails, phoney websites, and anonymous software are all available to buy on the web.

Even with advancements in technology on both sides of the fraud fence, an investigator with a good nose for a problem still plays an important role.

Complex fraud involves deception and concealment but this is just the seed – fraudulent activity still needs a fertile environment in order to germinate.

I have reflected on investigations completed by my team over recent years and these are my Top 10 current indicators of a fertile fraud environment.

## Top 10 indicators

- Organisations regularly undergoing periods of internal re-organisation. There's no better time for a fraudster to take advantage than when a restructure is underway.
- An unusually strong alliance with a single supplier in a highly competitive business area.
- Financial information becoming more complex and more difficult to understand, and taking longer to be produced.
- Suspense accounts that are miraculously zeroed just before year-end and the auditors' arrival.
- Employees promoted to manage senior technical areas without any sound financial/commercial experience.
- Contractors brought in to correct posting errors that the previous accountant never fixed before departing.
- Internal auditors are blocked from accessing the back-end system logs of the finance application by the IT department.
- Staff who password-protect and encrypt files on their My Documents folder.
- When the accounts payable master file has multiple entries for legitimate suppliers and everyone knows it needs “a good clean-up”.
- Executives who demand 24/7 access to the firm's electronic financial systems, yet the system records indicate they have never used them.



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

# Contacts



## 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) >

### 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)

**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 Sherrif - 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) >