McN+
McGRATHNICOL

ANZUIAG

Fraud and Forensic Accounting

10 November 2011

Dean Newlan

Partner

Overview

- Introduction to Forensic Accounting
- Real life fraud examples
- Key themes
- Interactive case study – Shepparton School of Agriculture
- Open forum

Forensic overview

	Dispute Advisory	Fraud and Corruption Investigation	Forensic Technology
Reactive	• Negligent act or omission • Breach of contract • Misleading and deceptive conduct • Trademark infringement • Business valuation	• Interview of suspects/ witnesses • Expert witness • Funds tracing/recovery • Discovery • Computerised charting • Quantification of loss	• Data recovery • Analysis of complex data • Expert witness • Email monitoring
Proactive	• Dispute avoidance • Assistance in mediation	• High level risk assessment • Detailed risk assessment • Fraud control planning • Integrity benchmarking	• Data mining • Penetration testing • Information systems risk assessment

Case study 1 – retail sector

How did it occur?	Substituted own bank account numbers in on-line banking system after processing but prior to authorisation. 95 transactions over two years. Debits charged to payroll clearing accounts. Periodic transfer out of clearing account to Trade Creditors Control to eliminate increasing debit balance.
How was it found?	Fresh copy of trade creditors sub-ledger printed in preparation for audit. Sub-ledger did not agree with control account.
What internal control failures allowed it to occur?	Lack of segregation of duty, poor control over on-line banking procedures, lack of review of journal postings.
Value of the loss suffered	$19.365 million
Consequential losses	Investigation / legal costs, management distraction.
What was the outcome?	Recovery of $16.5 million for the company, payroll manager sentenced to 5 years imprisonment.
Lessons learned	Tighter control over on-line banking systems and procedures, ensure segregation of duty, lock-down files so that only staff with a need can access financial information.

Case study 2 – non-bank financial institution

How did it occur?	Local manager of a remote office site falsified facsimile instructions to head office for payment of third party cheques. Cheques applied to own benefit. Manipulation of customer statements to restore account balance.
How was it found?	Client complaint to head office that there were no funds available in the account.
What internal control failures allowed it to occur?	Lack of head office monitoring of local operations, lack of routine analysis of redemption transactions, failure to send account statements directly to clients.
Value of the loss suffered	$6.2 million
Consequential losses	Investigation / legal costs, management distraction.
What was the outcome?	Recovery of amount stolen through insurance claim.
Lessons learned	Closer monitoring of remote operations, analytical analysis of redemptions relative to investments, ensure that statements of account activity are sent directly to clients.

Case study 3 – industrial markets manufacturer

How did it occur?	Transportation manager interposed bogus company between employer and service providers. Bogus company paid service providers and then billed employer adding 19% to the value of the genuine invoices paid.
How was it found?	Efficiency review identified unknown vendors.
What internal control failures allowed it to occur?	Poor control over registration of new vendors, lack of supervision of transactions by senior management
Value of the loss suffered	$2.05 million
Consequential losses	Investigation / legal costs, management distraction.
What was the outcome?	Recovery of amount stolen civil proceedings.
Lessons learned	Better control over vendor registration.

Key themes

- Breakdown in internal control (inadequate internal controls or poorly enforced internal controls)
- Trusted employee with significant access to payment systems who acted alone
- On-line banking a key risk
- Hiding the ‘debit’
- Failing to properly vet new vendors
- Swift action to secure assets assisted in recovery of funds stolen
- Use of civil procedures to locate and secure evidence
- Assistance to the police in order to ensure that investigation and prosecution is carried out on a timely basis

The common theme in all Forensic Accounting assignments …

‘A Focus on Evidence’

Types of evidence

- Oral testimony (viva voce evidence)
- Documents
- Accounting records
- Computer produced evidence
- Photographs
- Physical exhibits (e.g. cash, weapons, vehicles)

Contrasting the civil and criminal jurisdictions

	Criminal Jurisdiction	Civil Jurisdiction
Focus	Sees fraud as a crime against society	Sees fraud as a civil wrong (tort)
Parties	Director of Public Prosecutions -v- 'the accused'	Plaintiff -v-Defendant Applicant -v- Respondent
Objective	Deterrent to the general community, maintain order in society	Recovery of stolen property
Mode	Trial by Judge and Jury or trial by Magistrate	Trial by Judge alone
Standard of Proof	Beyond reasonable doubt	Balance of probabilities

Some useful civil procedure concepts

Discovery	Process ordered by the Court where the parties to litigation must disclose all relevant evidence to the other party in their possession including evidence that may be favourable to the other party
Non-party discovery	Discovery orders against a party who is not a party to the litigation (e.g. a bank) – generally can only used where the plaintiff is attempting to determine who can be sued or what cause of action their might be.
Subpoena	Order of the court to produce evidence to the court at or shortly prior to trial.
Anton Piller Order	Order of the court authorising a party to litigation to make a search of premises controlled by another party to the litigation. Generally will only be granted if can be established that normal process for party-party discovery has or is likely to fail.
Mareeva Injunction	Temporary freeze on dealing with assets. Must be able to "trace" the proceeds of criminal conduct or civil breach into the asset against which the order is sort.

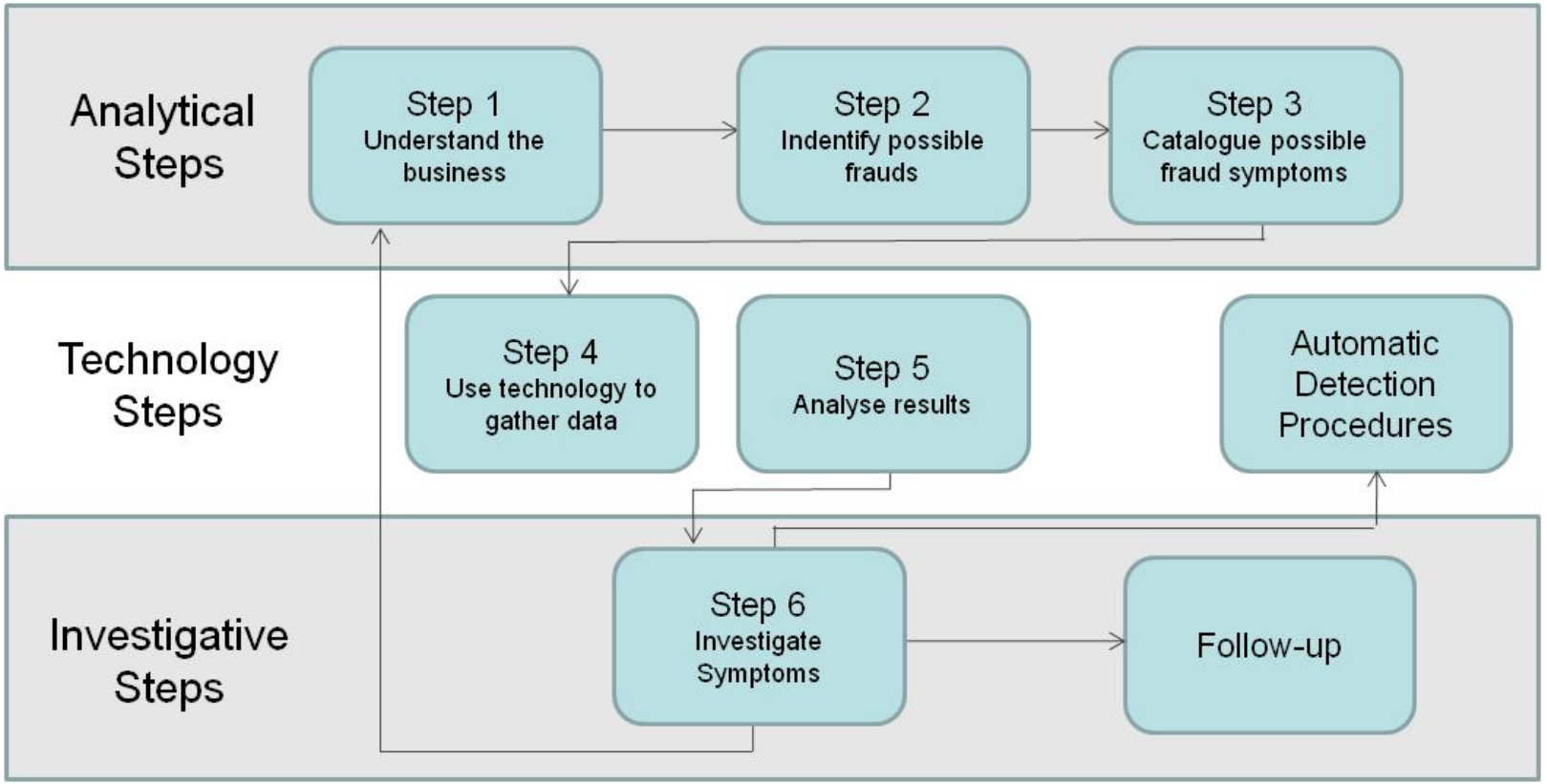
A four phased investigation program

Planning	Gather & secure evidence	Analyse evidence	Reporting
+ Agree objectives / scope + Form investigation team and brief team + Determine need for external resources + Develop schedule of required internal documentation + Develop schedule of required external documentation + Refine project methodology + Confirm reporting requirements + Document project plan and agree with the client	+ Identify and secure critical evidence + Identify and secure assets + Identify witnesses + Interview key individuals + Utilise Forensic Technology + Identify, gather and collate physical records + Conduct corporate intelligence of persons and corporations	+ Comparative analysis of all captured documentation, including communication records + Use forensic tools to interrogate records and identify misconducts or non-compliance patterns + Conduct further interviews of individuals + Prepare intelligence chart showing transactions, inter-relationships, flow of information or timeline + Interview individuals subject to allegations where appropriate	+ Prepare draft report and confer with the manager in charge – finalise report + Liaise with proper authorities (e.g. Police) + If warranted, prepare brief of evidence + Prepare and present expert testimony in court, tribunal or mediation as and if required + Quantify any loss suffered and liaise with insurer / loss adjustor etc

Fraud detection techniques

- Recognising typical symptoms (red flags) of fraud
  i.e. indicators that fraud may or is likely to have occurred
- The auditing of financial statements
- The use of financial statement analysis and other analytical methods
- The use of information technology tools (data analysis)

Effective data analysis



Data analysis routines

Fraud type	Potential data analysis that may identify indicators of fraud of this type
Accounts payable fraud (internally instigated)	• Matching bank account numbers of suppliers with staff – may indicate staff member has nominated payroll account to receive payment for fraudulently submitted invoices • Matching telephone numbers or addresses of suppliers with known staff details – may indicate involvement of staff in submitting false invoices
Payroll fraud	• Matching bank account numbers for more than one employee
Expense account fraud	• Duplicate invoice numbers or amounts – may suggest that the same invoice has been used to support more than one payment • Unusual frequency of expense claims of a particular type • Analysis of kilometres travelled claimed for reimbursement relative to the average
Financial statement fraud	• Identification of journal entries posted by personnel in unusual circumstances • Identification of unusual sale pattern immediately prior to balance date and possible reversal at the commencement of the next period

Case study

Shepparton School of Agriculture

Open Forum