RISQ GROUP

Now incorporating aim BACKGROUND SCREENING

Protecting Your Business From Fraud - Family Business Australia National Conference 2013

CASE STUDY

- Mobile phone store franchise
- Manager hired staff member with previous criminal history
- Additional staff hired with criminal history
- Phones and contracts entered into using fictitious ID
- Clawback in payments from telcos over $500k

CASE STUDY

- Transport company with sub-contracted drivers – high turn-over of employees
- Stolen Fuel cards from company vehicles used at local fuel station for unlawful purchases
- Poor security of fuel cards – hidden in vehicles
- Lack of audit on fuel use – only monthly
- Fuel Card PINs known to all drivers

CASE STUDY

- Construction company
- Project Manager purchased material used for personal projects using company account
- Poor audit of accounts – no job reference numbers attached to invoices
- Poor policy – Project Manager able to sign-off and authorise unlawful payments
- Project Manager had a history of fraud

CASE STUDY

- Material Supply Company
- Business Administrator arranged direct payments to her own account for jobs completed by the company
- No segregation of duties – only person to access and use accounts system and bank accounts
- Poor financial audit – did not detect missing funds for 2 years

The Facts

- “fraud occurs more often in family owned businesses….due to the trust factor…family members at family-owned business treat the business as though they are entitled to profit from it today.”
- “The family treats the business too informally because it’s run by family members and nobody wants to suggest they don’t trust one another.”

Professor Enrique Soriano – Family Business Forum, The Philippines, March 2013

The Facts

- “the major reason fraudsters can commit their crimes is because management trusts them so much: they’re family members or longtime friends, or they have proven work records and years of service.”

George Cassola, Managerial Auditing Journal, Volume 8, 1993, Issue 7

The Facts

- Median loss from fraud is USD140,000
- Organisations with less than 100 employees were most common to experience fraud (3.18%)
- 87% of fraudsters never been charged with fraud offence
- 41.5% of fraudsters had been with the organisation for between one and five years, had tertiary qualifications and worked in accounts area

Association of Certified Fraud Examiners 2012 Report to the Nations

What is Fraud?

- **Fraud** - ‘dishonestly obtaining a benefit by deception or other means’.
  - Tangible benefit (monetary/material)
  - Intangible (unauthorised access of information)
  - 3rd party may also ‘benefit’
  - mental element
  - internal fraud (employees, contractors) and external fraud (service providers, other)

Examples of Fraud

- misappropriation or misuse of funds by third parties;
- false invoicing or deficient supply of goods and services under contract;
- fraudulent claim or use of employment entitlements and expenses;
- theft or wrongful use of assets, equipment, facilities or services;
- collusion/misappropriation during procurement/divestment of goods and services;
- misappropriation in funds transfers;
- providing false or misleading information e.g.
  - making, using or possessing forged or falsified documents; and
  - tampering with or destroying records.

A member's personal experience

Ms Angela Ciliberto, C-Direct

Times of High Risk

- During periods of rapid growth – outpaces control environment, new staff, poor practices
- System changes – accounting, payroll, inventory control
- Tough financial times – financial pressure, reduced staff, lack of segregation of duties

Red Flags

- Failure to provide financial information
- Failure to co-operate with management
- Failure to take leave, early starter, late finisher
- Poor record keeping
- High staff turnover within a department
- Unexplained decline in cash flow
- Increase in payment terms

Key Controls

- Ethical culture – promoted through relevant policies, processes and management actions

TIP – “walk the talk”, use Fraud Policy, ongoing training, follow through on investigations.

- Effective security – personnel & physical security

TIP – Employment Screening (AS4811:2006), vendor due diligence, review of security controls, change passwords etc

Key Controls

- Training – increased awareness of fraud risks

TIP – provided during induction, ongoing, tailored.

- Detection of fraud – through auditing, fraud risk assessments

TIP – risk-based approach to audit, liaise with auditors on high risk areas, use of CAAT's

Key Controls

- Reporting – internally and externally

TIP – Trust your “gut instincts”, follow up on concerns/disclosures, use a hotline or other reporting channel

- Information Security – IT and IP

TIP – policies supported by training, disable external ports, understand what your IP is and is worth

Dealing with a fraud event

- Keep on a need to know basis
- Gather all relevant evidence – covert v overt
- Consider electronic sources – computers, server, access control, mobile phones, PABX
- Engage relevant stakeholders – legal, HR, head of dept
- Use appropriately qualified resources – experience in investigation, preparing briefs, interviewing
- DO NOT CONFRONT THE SUSPECT UNTIL EVIDENCE IS GATHERED

Dealing with a fraud event

INSURERS –

- Be aware of policy limit/excess/notification clause
- Comprehensive proof of loss – evidence and quantum

POLICE –

- Will require a brief of evidence
- Need to follow up regularly – importance/expertise

LAWYERS –

- Ensure you agree objectives – civil/criminal/assets/restitution
- Keep control of scope/costs
- Do as much as you can internally

Recovering from a fraud event

STAFF –

- Keep informed, as appropriate
- Provide training to prevent future occurrences

CUSTOMERS/SUPPLIERS –

- Have a consistent message
- Revisit agreements/contracts

MEDIA –

- Single point of contact
- Emphasise positives – eg. Quick detection, recovery of funds etc

Conclusion:

- All businesses are susceptible to fraud NOT ONLY family businesses
- Trust can be a double-edged sword – needs to be supported by strong control framework
- Look for "red flags" and trust your instincts
- Have a plan to respond to and recover from a fraud event

QUESTIONS?

Guy Underwood

Executive Chairman

The RISQ Group

E: guy.underwood@risqgroup.com

Ph: +613 9670 9855