Fraud – the enemy within

24 November 2017
The global profile of a fraudster
Development of Profiles of the fraudster

2010
348 cases in 69 countries

2013
596 cases in 78 countries

2016
750 cases in 81 countries
Focus on the 2016 Survey

2016

— 750 fraudsters from 81 countries. Up from 596 in prior survey.
— Frauds investigated from March 2013 to August 2016.
— Survey expanded to explore certain topics more deeply
— New in this survey— delved into technology (enabler and detector) and added a series of questions around the characteristics of the cyber-fraudsters.
Fundamental characteristics: Overview

- Well respected (38%), nearly 4x more likely than someone with a low reputation
- Autocratic, 3x more likely to be regarded as friendly as not
- Has a sense of superiority
- Has unlimited authority
- 65% of fraud lasted between 1 and 5 years

Type of Fraud:
- Misappropriation of Assets (47%);
- Financial reporting fraud (22%).

Cost of Fraud:
- Cost to company exceeding $1M (27%).

Holds an executive level position
- (34%) Manager (32%);
- Staff (20%)
Enablers: Weak controls

- Collusion circumventing good controls: 11%
- Reckless dishonesty regardless of controls: 21%
- Weak internal controls: 61%
- Other: 5%

Source: Global Profiles of the Fraudster, KPMG International, 2016
Enablers: Technology

Was technology used as an enabler to perpetrate the fraud?

- **16%** Yes, the fraud could not have been perpetrated without using technology
- **26%** Somewhat, but the fraud could likely have occurred without technology
- **47%** Technology was not used to enable the fraud

Source: Global Profiles of the Fraudster, KPMG International, 2016
Enablers: Technology (cont.)

- Created false or misleading information in accounting records: 24%
- Abused permissible access to organisation’s computer systems: 13%
- Provided false or misleading information via email or other messaging platform: 20%
- Obtained access to organisation’s computer systems without permission: 3%
- Other: 8%

Source: Global Profiles of the Fraudster, KPMG International, 2016
Means of detection

How were the Frauds detected?

- Tips offs and complaints, other than formal hotline: 24%
- Management review: 22%
- Formal whistle blowing report/hotline: 20%
- Accidental: 14%
- Internal audit: 14%
- Suspicious superior: 10%
- Other internal control: 7%
- External audit: 6%
- Self-reported/admitted: 3%
- Proactive fraud-focused data analytics: 3%

Source: Global Profiles of the Fraudster, KPMG International, 2016
Case studies
Categories of fraud

### Misappropriation of assets
- Payroll fraud
- Expenses fraud
- Procurement fraud
- Contractor fraud
- Theft of assets e.g. stock and cash
- Theft of intellectual property

### Fraudulent financial reporting
- Improper revenue recognition
- Overstatement of assets
- Understatement of liabilities
- Customer overbilling
- Treasury & investment related fraud

### Related illegal activity
- Anti-competitive behaviour
- Bribery and corruption
- Money laundering
- Organised crime
- Unethical behaviour
- Conflicts of interest
Case study 1: Conflicts of interest

Whistle-blower allegations

“The General Manager of the business awards all of the on site facilities management to his friend’s business and the company is paying too much money for this work.”

Findings

- The supplier was engaged by the company without a formal competitive tender process.

- There was no formal contract in place between the company and the supplier.

- The supplier’s prices were higher than those of its competitors.

- The General Manager was close friends with the owner of this supplier – they lived in the same village and had gone on a number of holidays together.
Case study 2: Revenue recognition

Whistle-blower allegation

“…fraudulent financial accounting and reporting, poor management of the business fundamentals.

We have a huge problem with our sales. We have a practice of shipping goods that the customer wants but many months in advance of the due date. We have even been shipping goods that the customer didn’t order at all. We have material debts building up and many of our customers have credit limits which are too high. Senior management override them. One of our teams is deliberately double invoicing and then withholding the credit notes.”

Findings

- Pressured sales-driven environment – “growth at any cost”.
- Abnormal year-end revenue spike.
- Large numbers of credit notes issued in Q1 of the following year.
- ‘Fictitious’ year-end sales.
- Issues with aged debtors.
Case study 3: Collusion

Whistle-blower allegation

“The Logistics Manager and General Manager are colluding with a local haulage business. The haulage company is submitting fictitious invoices for work which is never delivered and we are paying these invoices.”

Findings

- The Logistics Manager had manipulated records in the company’s logistics management system by adding in false shipments.

- The numbers for these fake shipments were provided to the supplier which subsequently issued fictitious invoices for these shipments.

- The Logistics Manager and the General Manager were the first and second level approvers respectively for the invoices submitted by this supplier, and they approved all of the fictitious invoices.

- The Logistics Manager had been subject to bankruptcy proceedings, which may have motivated him to engage in this scheme.
Red flags
Red flags: The employee

<table>
<thead>
<tr>
<th>Lifestyle / Income mismatch</th>
<th>Overextended personal finances</th>
<th>Addictive behaviour</th>
<th>Relationship “issues”</th>
<th>Rarely takes holidays</th>
</tr>
</thead>
<tbody>
<tr>
<td>Refuses or does not seek promotion</td>
<td>Resists or refuses new positions</td>
<td>Poor motivation or unhappy</td>
<td>Stressed, pressurised</td>
<td>Unreliable, prone to mistakes, poor performance</td>
</tr>
<tr>
<td>Shifts blame for errors, denies responsibility</td>
<td>Over secretive</td>
<td>Egotistic</td>
<td>Bullies or intimidates colleagues</td>
<td>Ability and performance not in tune with CV</td>
</tr>
<tr>
<td>Has favourites or is surrounded by “yes men / women</td>
<td>Personal pay and reward could be manipulated</td>
<td>Does not, or cannot produce notes or records of business meetings</td>
<td>Vendors and suppliers will not speak to anyone but this person</td>
<td>Cuts corners or bends the rules!</td>
</tr>
</tbody>
</table>

© 2017 KPMG International Cooperative (“KPMG International”) is a Swiss entity. Member firms of the KPMG network of independent firms are affiliated with KPMG International. KPMG International provides no services to clients. No member firm has any authority to obligate or bind KPMG International or any other member firm vis-à-vis third parties, nor does KPMG International have any such authority to obligate or bind any member firm.
Red flags: Procurement fraud

- Suppliers with limited history
- Complaints from other bidders
- Poor quality work
- Absence of policies and procedures
- Absence of formal written contracts and price lists
- High risk jurisdictions
- Related bidders
- Budget overspend
- Large number of invoices below specific approval thresholds
- Invoice payments with limited supporting documentation
- Changes of supplier information in SAP without written confirmation
- Inconsistent application of tender processes
- “We have always used them” attitude
- “Favourite” suppliers
- Lack of due diligence
- High number of contract change requests
- Bank accounts in offshore jurisdictions
- Bank accounts not in the same jurisdictions as countries of operation
- “It was a rush order”
- Single source contracts
# Red flags: Corporate

<table>
<thead>
<tr>
<th>Lack of trust / poor internal or external auditor relationship</th>
<th>Dominance / lifestyle issues</th>
<th>Undue secrecy</th>
<th>Illegal / unethical practices</th>
<th>Significant director share sales</th>
</tr>
</thead>
<tbody>
<tr>
<td>High analyst or other pressures</td>
<td>Declining industry / earnings</td>
<td>High hope value</td>
<td>Aggressive forecasts</td>
<td>Highly-leveraged rewards</td>
</tr>
<tr>
<td>Aggressive accounting policies</td>
<td>Unique products – unique risks</td>
<td>Cash / funding gap</td>
<td>Results exceed market trend</td>
<td>High management turnover</td>
</tr>
<tr>
<td>Profit warnings / credit warnings</td>
<td>Complex corporate structures</td>
<td>Related party arrangements</td>
<td>Multiple banking arrangements</td>
<td>Remote operations</td>
</tr>
</tbody>
</table>
Fraud prevention
# Fraud prevention: The building blocks

## Culture

A strong framework of policies and procedures are key to implementing and maintaining a robust anti-fraud framework and maintaining the right culture.

- Clear ‘tone from the top’;
- Introduce and/or implement relevant governance policies;
- Develop a clear code of conduct for your business;
- Develop your internal reporting procedures;
- Develop a robust fraud policy and response plan; and
- Review and develop

## Due diligence

An understanding of which parts of your business are most vulnerable to risk is essential in minimising risk of brand or reputational damage.

Do you really know who is working for you and who you are doing business with?

- Risk assessment programme;
- Undertake supply chain mapping and current state analysis;
- Risk rate third parties and develop mitigating actions;
- Conduct focused due diligence and adverse media reviews; and
- Conduct ongoing review and monitoring.

## Monitoring

Ensuring that your anti-fraud programme is embedded into business as usual and throughout the various operating models within the business.

- Stakeholder management;
- Implementation of policies and procedures and governance frameworks;
- Supplier development programme for all existing and new suppliers;
- Continuous monitoring; and
- Identify relevant KPIs to monitor compliance and

## Closing the loop

Should issues be identified, ensure you have an appropriate plan in place to identify, address and remediate issues.

- Effective management of potential issues;
- Investigation and appropriate follow up action;
- Reporting to senior management and the Board;
- Prepare a detailed remediation plan;
- “Join the dots”; and
- Revisit the site on a timely basis.
Thank you
Nicola Cobb –
Director, Forensic
0207 311 3792
Nicola.cobb@kpmg.co.uk