Contents

Introduction .......................................................................................................................... 3
Executive summary ............................................................................................................. 4
About this research ............................................................................................................ 5
  Aim of the research ......................................................................................................... 5
  How the research was undertaken .................................................................................. 5
Amounts stolen .................................................................................................................. 6
The perpetrators ................................................................................................................ 7
  Sex ..................................................................................................................................... 7
  Age ..................................................................................................................................... 7
  Role .................................................................................................................................... 8
  Prior criminal history ....................................................................................................... 8
  Was there collusion involved? ......................................................................................... 8
How were the frauds committed? ....................................................................................... 9
Where were the frauds perpetrated? .................................................................................. 10
Fraud by industry .............................................................................................................. 11
Duration of frauds ............................................................................................................ 12
How were the frauds discovered? ..................................................................................... 13
Warning signs that were ignored ...................................................................................... 15
What was the motivation? ................................................................................................. 16
  Gambling as a motivator ................................................................................................. 17
  Lifestyle as a motivator ................................................................................................. 18
Impact of the frauds on the victims .................................................................................. 19
Impact of the frauds on the perpetrators .......................................................................... 20
  Sentences ........................................................................................................................ 20
  Recompense and financial burden ................................................................................ 20
  Other impacts ................................................................................................................ 21
Contact us ........................................................................................................................ 22
Introduction

When an organisation loses more than a million dollars to an act of fraud, questions are asked. How did it happen? What is the size of the fraud? Who is involved? Why didn’t our internal controls pick it up more quickly? Can we recover the losses?

Board members and senior management will demand answers. On occasions, the person or persons who committed the fraud may be amongst the senior managers.

The investigation costs, legal expenses and management time lost as a result of conducting and monitoring the progress of the investigation and dealing with stakeholders can be significant. In the case of fraud on banks, financial advisory firms and funds managers, their clients may have concerns over the governance of the organisation to protect their assets.

This research looks at million dollar frauds in recent history in Australia that have been perpetrated by employees.

The research does not include frauds perpetrated on clients by accountants, lawyers or investment advisors. It does not include taxation fraud or welfare fraud. Nor does it include frauds perpetrated on financial institutions by its customers or other third parties such as identity theft or mortgage fraud. It focuses exclusively on acts of fraud committed by management and staff of organisations, whether they are public or private companies, not for profit, associations, government or professional organisations.

It covers the period 1 January 2001 to 31 July 2012. To be included in the research, the fraud must have satisfied the following criteria:

• The amount stolen had to exceed AUD1 million dollars.

• The fraud resulted in a criminal conviction in an Australian court of law during this period for an offence that falls under the general umbrella of ‘fraud’.

• The fraud had been perpetrated by an employee or employees.

This is the fourth major fraud research study undertaken by Warfield & Associates since 2008.

We trust this new fraud research can assist organisations understand that they need to be proactive with regard to fraud control and learn from the mistakes of others!

Brett Warfield
Partner
Warfield & Associates
August 2012
Executive summary

The key findings of the research include:

- 89 cases were identified involving 93 employees.
- 66 of the 93 perpetrators were male and 27 were female.
- Perpetrators ranged in age from 24 to 67 years old.
- At least seven perpetrators had prior criminal histories for deception related offences.
- $398 million was stolen.
- Nine cases involved at least $10 million being stolen.
- The largest amount stolen by an employee was $45.3 million.
- The banking sector was the hardest hit with 30 frauds. This was more than a third of all cases.
- Every person included in this research was sentenced to a gaol term.
- In two cases, offenders received a gaol sentence of only six months non-parole.
- Gambling addiction was the main motivating factor in 46 of the cases. This is more than half the cases in the research.
- 43 cases involved employees transferring some, or all, of the fraudulently obtained funds to their own bank accounts by Electronic Funds Transfer. With cheques being phased out by businesses, more Electronic Funds Transfer crime will occur in the future.
- Victoria had more than 1/3 of all frauds yet NSW incurred the biggest losses totaling $153 million.
- Accountants and Bookkeepers were the most prevalent job titles of the perpetrators.
- Of the 62 employees who committed fraud against organisations other than banks, 38 were employed in the finance department.
- Only nine of the cases involved collusion with another person or persons.
- 40 of the frauds took more than five years to discover.
- In many cases it is clear that a forensic audit of key areas would have prevented frauds from continuing.
- The duration of time taken to discover frauds should be of real concern to those responsible for governance in their organisations. No organisation can completely stop fraud from happening. However, a number of these organisations had large frauds occurring that were not discovered by their internal controls and reviews over what can only be regarded as an incomprehensible period of time.
- It is clear that educating staff about the warning signs of fraud and basic fraud risk mitigation strategies have been absent in most cases. Training staff in what to look for and identifying the ‘Red Flags’ of fraud is an invaluable fraud mitigation and detection tool. All organisations, regardless of size, should consider fraud awareness training.
About this research

Aim of the research

This report presents the findings of a 2012 Australia-wide study into fraud perpetrated by employees.

The aim of this research is to increase existing knowledge about the impact of those who betray trust and to provide guidance for organisations as to how to reduce the incidence of this type of crime in the future.

It is by improving awareness of how other organisations have suffered and the lessons they have learnt, that an organisation can become more proactive and put in place preventative and detective measures that mitigate the extent and impact of fraud.

How the research was undertaken

The research for this study involved an extensive review of online law judgements, as well as Australian newspaper articles containing court reports that provided details of judgements.

The relevant period covered by the research was any conviction in an Australian court of law during the period 1 January 2001 to 31 July 2012, for deception related offences, where evidence was led that the perpetrator was an employee and the amount stolen was in excess of $1 million.

Examples of the types of criminal offences that were included in the research included, but were not limited to:

- Embezzlement
- False accounting
- Falsification of accounts
- Forgery
- Fraudulent misappropriation
- Larceny by a clerk
- Make false document
- Make false instrument
- Making false entries
- Obtain property by deception
- Obtaining financial advantage by deception
- Stealing as a servant
- Theft
- Use false document
- Uttering
Amounts stolen

89 cases were included in the study with a total amount stolen of $1 million or more over the research period. This represented an average of $4,472,204 per fraud.

The five largest frauds included in the research involved amounts of $45.3 million, $27.3 million, $22.4 million, $19.3 million and $19 million.

Some may think it is quite extraordinary that, in most cases, a single employee could undertake such deception without being identified by internal controls, management oversight, internal and external audit or even chance for so long.

Some organisations can withstand a large fraud. They have the economic resources to recover, whether it is through taking expensive legal action against the perpetrator, claiming on their insurance policy or simply writing off the amount. For small to medium sized organisations, the impact can be far greater and, on occasions, lead to the closure of the business.

### Figure 1 – Amounts defrauded by range

<table>
<thead>
<tr>
<th>AMOUNT DEFRAUDED</th>
<th>NUMBER</th>
<th>AMOUNT</th>
</tr>
</thead>
<tbody>
<tr>
<td>Over $20 million</td>
<td>3</td>
<td>$95,169,652</td>
</tr>
<tr>
<td>$15 million to $19,999,999</td>
<td>4</td>
<td>$71,065,000</td>
</tr>
<tr>
<td>$10 million to $14,999,999</td>
<td>2</td>
<td>$20,570,420</td>
</tr>
<tr>
<td>$5 million to $9,999,999</td>
<td>10</td>
<td>$69,985,071</td>
</tr>
<tr>
<td>$1 million to $4,999,999</td>
<td>70</td>
<td>$141,236,000</td>
</tr>
<tr>
<td><strong>Totals</strong></td>
<td><strong>89</strong></td>
<td><strong>$398,026,143</strong></td>
</tr>
</tbody>
</table>

Case Study 1

**Amount stolen:** $16.7 million

**Motivation:** Lifestyle

**Industry sector:** Retail

**Sentence:** Six and a half years gaol with a non-parole period of four years

**Details:** Male, in early 40s, created false invoices and disguised the financial hole they created by setting budgets high enough to include such amounts. Misappropriated money over a five year period. Money was frittered away on keeping his private businesses afloat as well as ‘keeping up with the Joneses’ in his highly competitive eastern suburbs social circle. Only $50,000 was recovered when his family home was auctioned.
The perpetrators

Sex

There were 93 perpetrators involved in the 89 frauds included in the research.

71% of the offenders were male.

![Figure 2 – Total fraud by sex](image)

The largest single fraud in the study of $45.3 million was perpetrated by a woman. This has certainly impacted the averages for all women.

Eight men and two women were responsible for the ten largest amounts stolen.

Age

The age of the perpetrators as at conviction and/or sentencing has been used as the reference point. The youngest perpetrator was 24 and the oldest was 67. Where there were two perpetrators involved, the amount stolen was averaged between the two age groups. The following table breaks down the age groups.

<table>
<thead>
<tr>
<th>AGE GROUP</th>
<th>NUMBER</th>
<th>AMOUNT</th>
<th>AVERAGE</th>
</tr>
</thead>
<tbody>
<tr>
<td>Under 31</td>
<td>7</td>
<td>$23,858,238</td>
<td>$3,408,320</td>
</tr>
<tr>
<td>31-40</td>
<td>33</td>
<td>$176,877,910</td>
<td>$5,359,937</td>
</tr>
<tr>
<td>41-50</td>
<td>36</td>
<td>$156,413,054</td>
<td>$4,344,807</td>
</tr>
<tr>
<td>51-60</td>
<td>12</td>
<td>$27,821,067</td>
<td>$2,318,422</td>
</tr>
<tr>
<td>61-70</td>
<td>5</td>
<td>$13,055,874</td>
<td>$2,611,175</td>
</tr>
<tr>
<td><strong>Total 93</strong></td>
<td><strong>93</strong></td>
<td><strong>$398,026,143</strong></td>
<td><strong>$4,279,851</strong></td>
</tr>
</tbody>
</table>

![Figure 3 – Fraud by age groups](image)
Role

The perpetrators were identified by a job title and their basic responsibilities. In most organisations, senior management have significant delegation to authorise large transactions and negotiate major agreements. Their delegation levels are higher than most other staff. The expectation is that with a higher level of seniority comes a greater degree of trust.

However, those in the finance and accounting functions also can be given significant responsibility for organising and approving cheque payments and authorising payments by Electronic Funds Transfers.

Of the 62 employees who committed fraud against organisations other than banks, 38 were employed in the finance department.

With the exception of the bank specific role of bank manager, the most common job titles were all finance related.

The most common job titles were as follows:

<table>
<thead>
<tr>
<th>JOB TITLE</th>
<th>NUMBER</th>
<th>AMOUNT</th>
<th>AVERAGE</th>
</tr>
</thead>
<tbody>
<tr>
<td>Accountants</td>
<td>9</td>
<td>$84,225,320</td>
<td>$9,358,369</td>
</tr>
<tr>
<td>Bookkeepers</td>
<td>8</td>
<td>$16,916,631</td>
<td>$2,114,579</td>
</tr>
<tr>
<td>Bank Managers</td>
<td>8</td>
<td>$42,082,737</td>
<td>$5,260,342</td>
</tr>
<tr>
<td>Financial Controllers</td>
<td>7</td>
<td>$31,822,527</td>
<td>$4,546,075</td>
</tr>
<tr>
<td>Payroll Officers</td>
<td>6</td>
<td>$10,535,866</td>
<td>$1,755,978</td>
</tr>
<tr>
<td>Accounts Clerks</td>
<td>5</td>
<td>$8,410,484</td>
<td>$1,682,097</td>
</tr>
</tbody>
</table>

*Figure 4 – Most common job titles*

Prior criminal history

Of the 93 perpetrators in the 89 cases, seven had prior criminal histories for deception related offences. However, one of those went back 20 years and therefore, may not have been identified in even the most robust employment screening process.

In total, the seven perpetrators were responsible for frauds which totalled $13,090,000.

Background checking / pre-employment screening processes have become more prevalent over the past decade. Many organisations are requiring criminal record searches be undertaken on some, or all, of their prospective employees.

Was there collusion involved?

There were nine cases of collusion. Four involved collusion with a fellow staff member and the remaining five were assisted by external people to commit the frauds.

To be identified as a person/persons colluding with the employee/s, the collusion had to be overt. This meant they actively assisted with the fraud as opposed to being just the owner of a bank account into which the funds were transferred.

It is clear that other staff may have inadvertently been involved in the frauds, such as processing the transactions at the request of the perpetrator, though not knowing they were illegitimate transactions. However, where this was unknowing, they were not regarding as actively colluding.

The fact that 90% of the perpetrators of the frauds acted alone is consistent with other fraud research and surveys reporting on internal fraud.
How were the frauds committed?

In 43 cases the perpetrators transferred some, or all, of the fraudulently obtained funds to their own bank accounts via the Electronic Funds Transfer (EFT) system.

The increased use of Electronic Funds Transfer by businesses to pay creditors and staff will no doubt place greater responsibility in the hands of staff. Unless there are adequate controls over the Electronic Funds Transfers, this type of fraud will only grow in number and size in the future.

We believe that if one lesson is learnt from this research, it is that organisations must ensure the controls over their Electronic Funds Transfers are regularly reviewed by those with a good understanding of how the systems can be manipulated.

Just as Electronic Funds Transfer fraud will continue to grow, cheque fraud will diminish as more and more businesses pay their staff and creditors by funds transfer. The Australian Payments Clearing Association website records that the volume of cheque payment transactions has halved in the period 2007 to 2012 from 40.3 million transactions per month to 21 million.

Fraudulent loans and stealing from a customer’s bank account were all perpetrated against banks by their staff members. These included creating false names and addresses or establishing loans in the names of existing customers without their knowledge.

In most cases, the cheque frauds were carried out by simply falsifying a signature or signatures on company cheques. Many of these were made out to ‘cash’.

False invoicing continues to be a prevalent method of fraud. Invoices are created for goods or services that have either never been rendered, or for which the fees have been greatly exaggerated. One example included setting up a consulting company in a false name and making payments to it. Another involved inflating 49 invoices for construction work, on some occasions in the order of 500 per cent.

<table>
<thead>
<tr>
<th>METHOD</th>
<th>NUMBER</th>
<th>AMOUNT</th>
<th>AVERAGE</th>
</tr>
</thead>
<tbody>
<tr>
<td>EFT to own bank account</td>
<td>18</td>
<td>$81,648,391</td>
<td>$4,536,022</td>
</tr>
<tr>
<td>Fraudulent loans</td>
<td>12</td>
<td>$34,107,649</td>
<td>$2,842,304</td>
</tr>
<tr>
<td>Cheque fraud</td>
<td>11</td>
<td>$33,415,988</td>
<td>$3,037,817</td>
</tr>
<tr>
<td>False invoicing</td>
<td>11</td>
<td>$50,674,429</td>
<td>$4,606,766</td>
</tr>
<tr>
<td>Stole from customer’s bank accounts</td>
<td>10</td>
<td>$40,109,169</td>
<td>$4,010,917</td>
</tr>
<tr>
<td>EFT to own bank account and other third parties</td>
<td>8</td>
<td>$96,383,077</td>
<td>$12,047,885</td>
</tr>
<tr>
<td>Payroll fraud</td>
<td>4</td>
<td>$6,935,866</td>
<td>$1,733,967</td>
</tr>
<tr>
<td>Multiple frauds used</td>
<td>4</td>
<td>$15,879,652</td>
<td>$3,969,913</td>
</tr>
<tr>
<td>Diversion of revenue</td>
<td>3</td>
<td>$6,652,500</td>
<td>$2,217,500</td>
</tr>
<tr>
<td>Fraudulent transfers to third parties</td>
<td>2</td>
<td>$20,000,000</td>
<td>$10,000,000</td>
</tr>
<tr>
<td>Cheque and EFT fraud</td>
<td>2</td>
<td>$3,838,598</td>
<td>$1,919,299</td>
</tr>
<tr>
<td>Theft of stock / inappropriate write-off</td>
<td>1</td>
<td>$1,000,000</td>
<td>$1,000,000</td>
</tr>
<tr>
<td>Fraudulent tax returns</td>
<td>1</td>
<td>$1,127,304</td>
<td>$1,127,304</td>
</tr>
<tr>
<td>False insurance claims</td>
<td>1</td>
<td>$4,328,520</td>
<td>$4,328,520</td>
</tr>
<tr>
<td>Tender fraud</td>
<td>1</td>
<td>$1,925,000</td>
<td>$1,925,000</td>
</tr>
<tr>
<td></td>
<td>89</td>
<td>$398,026,143</td>
<td></td>
</tr>
</tbody>
</table>

Figure 5 – Method of fraud

Where were the frauds perpetrated?

The frauds were broken down by State and Territory in which they occurred. Victoria had the most frauds by number - 33, however NSW had the greater value of losses at $153.4 million.

The average for South Australia was significantly affected by having two very large frauds during the research period. In fact, both were in the top five largest frauds by value.

<table>
<thead>
<tr>
<th>STATE / TERRITORY</th>
<th>NUMBER</th>
<th>AMOUNT</th>
<th>AVERAGE</th>
</tr>
</thead>
<tbody>
<tr>
<td>Australian Capital Territory</td>
<td>4</td>
<td>$12,850,000</td>
<td>$3,212,500</td>
</tr>
<tr>
<td>New South Wales</td>
<td>25</td>
<td>$153,462,484</td>
<td>$6,138,499</td>
</tr>
<tr>
<td>Northern Territory</td>
<td>2</td>
<td>$3,480,000</td>
<td>$1,740,000</td>
</tr>
<tr>
<td>Queensland</td>
<td>14</td>
<td>$43,432,363</td>
<td>$3,102,312</td>
</tr>
<tr>
<td>South Australia</td>
<td>5</td>
<td>$55,502,403</td>
<td>$11,100,481</td>
</tr>
<tr>
<td>Tasmania</td>
<td>2</td>
<td>$2,424,658</td>
<td>$1,212,329</td>
</tr>
<tr>
<td>Victoria</td>
<td>33</td>
<td>$102,255,773</td>
<td>$3,098,660</td>
</tr>
<tr>
<td>Western Australia</td>
<td>4</td>
<td>$24,618,462</td>
<td>$6,154,616</td>
</tr>
<tr>
<td></td>
<td>89</td>
<td><strong>$398,026,143</strong></td>
<td></td>
</tr>
</tbody>
</table>

*Figure 6 – Frauds broken down by state and territory*

Case Study 2

**Amount stolen:** $1.8 million  
**Motivation:** To stop her four struggling businesses going bust  
**Industry sector:** Motor vehicle repairs  
**Sentence:** Ten years gaol with a non-parole period of four years  
**Details:** Female, aged 30, was trusted bookkeeper at a panel shop business where she siphoned off $1.8 million from the shop’s bank account over a period of 6 years. She used the money to prop up her own four local, struggling businesses which eventually all went bust. Over the period of time the fraud took place, the owner of the panel shop had to sack staff and move to a smaller premises but still debts mounted. The fraud came to light after the books didn’t add up and secret accounts in the perpetrator’s name were found to be draining money from the business. None of the money was recovered.
Fraud by industry

The financial services sector was hit heavily by frauds in the research period. 30 of 33 were banks. Five of the banks were hit at least three times during the period of the research with one bank being subject to million dollar frauds by employees on at least seven occasions.

<table>
<thead>
<tr>
<th>INDUSTRY</th>
<th>NUMBER</th>
<th>AMOUNT</th>
<th>AVERAGE</th>
</tr>
</thead>
<tbody>
<tr>
<td>Banks</td>
<td>30</td>
<td>$184,124,601</td>
<td>$6,137,487</td>
</tr>
<tr>
<td>Education and Training</td>
<td>2</td>
<td>$29,074,903</td>
<td>$14,537,452</td>
</tr>
<tr>
<td>Government</td>
<td>10</td>
<td>$24,519,708</td>
<td>$2,451,971</td>
</tr>
<tr>
<td>Legal Firms</td>
<td>2</td>
<td>$4,500,000</td>
<td>$2,250,000</td>
</tr>
<tr>
<td>Manufacturing</td>
<td>5</td>
<td>$9,101,652</td>
<td>$1,820,330</td>
</tr>
<tr>
<td>Mining</td>
<td>3</td>
<td>$4,988,753</td>
<td>$1,662,918</td>
</tr>
<tr>
<td>Motor Vehicle Dealers</td>
<td>3</td>
<td>$4,395,889</td>
<td>$1,465,296</td>
</tr>
<tr>
<td>Not For Profit</td>
<td>4</td>
<td>$7,870,000</td>
<td>$1,967,500</td>
</tr>
<tr>
<td>Other Financial Institutions</td>
<td>4</td>
<td>$15,422,801</td>
<td>$3,855,700</td>
</tr>
<tr>
<td>Recruitment / Employment</td>
<td>2</td>
<td>$6,300,000</td>
<td>$3,150,000</td>
</tr>
<tr>
<td>Retail</td>
<td>4</td>
<td>$41,523,353</td>
<td>$10,380,838</td>
</tr>
<tr>
<td>Transport</td>
<td>2</td>
<td>$26,989,061</td>
<td>$13,494,531</td>
</tr>
<tr>
<td>Wholesale</td>
<td>3</td>
<td>$5,300,000</td>
<td>$1,766,667</td>
</tr>
<tr>
<td>Other</td>
<td>15</td>
<td>$33,915,422</td>
<td>$2,261,028</td>
</tr>
<tr>
<td><strong>89</strong></td>
<td></td>
<td><strong>$398,026,143</strong></td>
<td></td>
</tr>
</tbody>
</table>

*Figure 7 – Frauds by industry*

**Case Study 3**

**Amount stolen:** $22.4 million  
**Motivation:** Gambling  
**Industry sector:** Transport  
**Sentence:** 14 years gaol with a non-parole period of nine years and six months  
**Details:** Male, aged 41, was employed as Financial Controller and Company Secretary for a transport company. In this role he was given autonomy and privileges which included the ability to act as a signatory to the bank accounts operated by the business. In the five months leading up to his arrest he stole and transferred $11 million plus into his bookmaker’s account. He also bought a luxury apartment and a $70,000 BMW.
Duration of frauds

The longest period a fraud went undetected was for an extraordinary 16 years, involving nearly $3 million being stolen from a bank. The next four longest periods of time to discover the frauds included just under 16 years, ten years, nine years two months and nine years.

Three of the frauds took more than ten years to discover.

The duration of time taken to discover frauds should be of real concern to those responsible for governance in their organisations. No organisation can completely stop fraud from happening. However, a number of these organisations had large frauds occurring that were not discovered by their internal controls and reviews over what can only be regarded as an incomprehensible period of time.

Management may want to believe that, in the event of fraud in their organisations, the internal controls will identify the issue fairly quickly. The evidence from the research clearly contradicts that assertion. The question that is apparent with a large number of the frauds committed by employees is, why did it take so long to discover?

The longer the period of time that the fraud goes undetected, the greater the impact on the person who commits the fraud and the organisation they defrauded. This is clearly evident in the above table.
How were the frauds discovered?

There were 61 cases where evidence of how the frauds were discovered was available. Not all were specific. 24 of the 61 referred only to an internal discovery. There was insufficient information provided to draw a conclusion in another 28 instances.

It has been recognised in previous surveys of fraud that it is only when a fraudster's routine is affected that many internal frauds come to light. There were at least 13 specific references to the frauds being discovered whilst the perpetrator was on leave or after they had left the organisation.

One of the most effective ways to mitigate the risk of fraud in an organisation is to educate staff about fraud and how it occurs. In particular, the warning signs that it may be happening.

Organisations should consider providing fraud awareness training to their staff to increase the likelihood frauds are identified more quickly.

Specific examples of the ways the frauds were discovered included:

- When cheques were dishonoured
- Customer could not withdraw funds from her account
- Anonymous letter
- Retailer contacted perpetrator’s employer concerning her ability to pay for luxury purchases
- Discovery of a forged cheque led to an audit
- Woman questioned the bank as to why she was being sent statements for a loan she did not arrange
- Referral from Star City to AUSTRAC concerning bets made by a gambler
- Bank alerted the company to a suspicious transaction
- Colleague noticed a duplicate payment
- Boss saw photo in the paper alerting him to the employee’s gambling habit
- Turned herself in after her son questioned her about an unusual bank account
- Bank notified company of its concerns regarding suspect transactions

---

**Case Study 4**

**Amount stolen:** $19.3 million

**Motivation:** Got a buzz from negotiating and dealing with real estate agents

**Industry sector:** Retail

**Sentence:** Eight years gaol with a non-parole period of five years

**Details:** Female, aged 39, was a Senior Accountant for a retailer. Over a period of two years she stole more than $19 million. In her capacity as a cheque signatory on the company’s bank account and also as one of two employees able to process Electronic Fund Transfers on the company’s behalf, she transferred payments from the company’s accounts into accounts controlled by her. With these funds she purchased 44 properties and two cars. Her fraud, in part, led to the collapse of the company.
Where the method of discovery was discussed, it has been incorporated into the table below. The exact method was not always revealed. Hence there are 24 instances referred to as being discovered internally. These were staff who found the fraud by various means. They may also be referred to as ‘Internal Controls’.

<table>
<thead>
<tr>
<th>HOW DISCOVERED</th>
<th>INSTANCES</th>
</tr>
</thead>
<tbody>
<tr>
<td>Administrator / Liquidator</td>
<td>2</td>
</tr>
<tr>
<td>After they left the job</td>
<td>8</td>
</tr>
<tr>
<td>Anonymous report</td>
<td>1</td>
</tr>
<tr>
<td>Bank notified organisation</td>
<td>4</td>
</tr>
<tr>
<td>Confessed</td>
<td>5</td>
</tr>
<tr>
<td>Customer / Client notified organisation</td>
<td>3</td>
</tr>
<tr>
<td>External Audit</td>
<td>1</td>
</tr>
<tr>
<td>External Forensic Accountants</td>
<td>2</td>
</tr>
<tr>
<td>Internal discovery by staff</td>
<td>24</td>
</tr>
<tr>
<td>When on leave</td>
<td>5</td>
</tr>
<tr>
<td>Other external party</td>
<td>6</td>
</tr>
<tr>
<td><strong>Total</strong></td>
<td><strong>61</strong></td>
</tr>
</tbody>
</table>

**Figure 9 – How frauds were discovered**

**Case Study 5**

**Amount stolen:** $45.3 million

**Industry sector:** Banking

**Motivation:** To fund a lavish shopping habit / revenge against employer

**Sentence:** 15 years gaol with a non-parole period of seven years

**Details:** Female, aged 40, managed to siphon off funds from the financial group she worked for to the tune of $45 million. She had worked for the company for over 20 years and at the time of her arrest held the role of Senior Accountant. She was able to commit fraud without being detected for a number of years and it was her own financial institutions that became suspicious of the money she was spending and made enquiries which led to the fraud being uncovered. During her shopping sprees she bought seven Sydney properties as well as jewellery from high end brands such as Paspaley, Chanel and Bulgari. She also loaned large amounts of money to people she hardly knew including $1.3 million to a staff assistant at one of the stores she frequented.
Warning signs that were ignored

The following warning signs or ‘red flags’ were ignored by the organisations subject to the frauds:

- Heroin and gambling addictions
- Retrenched but volunteered to keep working for no pay
- Promised clients higher interest rates to not touch their money
- When customers queried the shortfalls he told them a mistake had been made
- Lack of supervision and also needed no countersigning authorisation when ordering cash
- Regularly re-opened completed insurance claim files
- He set the budgets high so the spending was within budgets
- Inflated invoices for construction work, on some occasions in the order of 500 per cent
- No background check done on him. He had three prior convictions for gambling related fraud
- Instructed co-worker to alter documents so that stock meant for sale was deemed unsuitable
- Organised functions for cash
- Had responsibility for mail, book entries, presenting invoices for the Managing Director to sign, drawing cheques and telephone banking
- Never took more than a week off work at a time because irregularities would have shown up in the payroll
- Ignored company policy of staff not being allowed to arrange/approve loans to themselves and families or order loans in excess of $250,000
- Reactivated the accounts of a number of former employees no longer with the company and altered their bank details
What was the motivation?

It is often unclear what has really motivated a person to commit fraud. Sometimes there is clear evidence of asset accumulation, lifestyle choices or a gambling addiction. Based on evidence provided to the courts, we have tried to identify the motivation in each case. Lifestyle improvement and gambling were equally prevalent as the main reason the frauds were committed. Even when assessing some frauds that appear to be motivated by lifestyle, there were clear indications of much more deep seated emotional and psychological issues that resulted in the irrational behaviour. No better example of this relates to the largest fraud included in the research which exceeded $45.3 million. In this case the judge referred to these issues leading to resentment towards the company and a desire for revenge, as well as a range of personal issues.

<table>
<thead>
<tr>
<th>MOTIVATING FACTORS</th>
<th>NUMBER</th>
<th>AMOUNT</th>
<th>AVERAGE</th>
</tr>
</thead>
<tbody>
<tr>
<td>Gambling</td>
<td>46</td>
<td>$164,294,786</td>
<td>$3,571,626</td>
</tr>
<tr>
<td>Improve lifestyle*</td>
<td>35</td>
<td>$191,366,858</td>
<td>$5,467,625</td>
</tr>
<tr>
<td>Prop up failing businesses</td>
<td>3</td>
<td>$7,209,824</td>
<td>$2,403,275</td>
</tr>
<tr>
<td>Drugs</td>
<td>2</td>
<td>$4,500,000</td>
<td>$2,250,000</td>
</tr>
<tr>
<td>Investing on organisation’s behalf</td>
<td>2</td>
<td>$28,354,903</td>
<td>$14,177,452</td>
</tr>
<tr>
<td>Revenge</td>
<td>1</td>
<td>$2,299,772</td>
<td>$2,299,772</td>
</tr>
<tr>
<td></td>
<td>89</td>
<td>$398,026,143</td>
<td></td>
</tr>
</tbody>
</table>

* Note that in the largest single case in this study, the perpetrator raised the issue of revenge as a motivating factor for the fraud. However, the motivation was recorded as lifestyle due to the properties and luxury products that were purchased with the funds.

**Case Study 6**

- **Amount stolen:** $27.3 million
- **Industry sector:** Education
- **Motivation:** Lifestyle / Investing / Assisting others
- **Sentence:** Nine years gaol with non-parole period of five years and six months
- **Details:** Male, in his mid 40s, transferred funds into his personal bank accounts by having knowledge of two passwords. Started misappropriating funds six months into his employment at the University and continued for two years. Purchased a luxury home for his family, contributed funds to a sporting team and invested the bulk of the money. Less than $1 million was unrecovered. However, substantial legal and investigation expenses were incurred.
Gambling as a motivator

More than half the frauds in this research were motivated by a gambling addiction.

In order to understand what forms of gambling were most attractive to the perpetrators, an analysis was undertaken of the modes of gambling.

In the majority of cases, there was evidence that one main preferred gambling mode was used. On occasions, multiple gambling modes were identified to the courts.

Although it is recognised that the entire proceeds of the frauds would not have been spent gambling in every case, the overwhelming evidence in the cases that were reviewed was that the addiction resulted in not only most of the fraudulent proceeds being gambled, but also other income and family assets, resulting in little evidence of lavish lifestyle or asset accumulation.

In cases where gambling was a factor but the court judged the gambling not to be the main source of the problem and/or the use of the funds, these cases were not included as having a gambling motivation.

<table>
<thead>
<tr>
<th>MODE OF GAMBLING</th>
<th>NUMBER</th>
<th>AMOUNT</th>
<th>AVERAGE</th>
</tr>
</thead>
<tbody>
<tr>
<td>Poker machines</td>
<td>13</td>
<td>$35,008,017</td>
<td>$2,692,924</td>
</tr>
<tr>
<td>Casinos*</td>
<td>5</td>
<td>$19,321,761</td>
<td>$3,864,352</td>
</tr>
<tr>
<td>Horseracing</td>
<td>8</td>
<td>$62,798,110</td>
<td>$7,849,764</td>
</tr>
<tr>
<td>Internet Sports Gambling</td>
<td>1</td>
<td>$1,530,000</td>
<td>$1,530,000</td>
</tr>
<tr>
<td>Other (Lotto, TAB, Cards, Dogs, Online gambling, Offshore betting, Sports betting, Poker, Football pools, Lotteries, and multiples of any of the above modes)</td>
<td>11</td>
<td>$29,710,603</td>
<td>$2,700,964</td>
</tr>
<tr>
<td>Unknown</td>
<td>8</td>
<td>$15,926,295</td>
<td>$1,990,787</td>
</tr>
<tr>
<td><strong>Total</strong></td>
<td>46</td>
<td><strong>$164,294,786</strong></td>
<td></td>
</tr>
</tbody>
</table>

* This excludes references to poker machines played at a casino, which have been included in the poker machine figures.

Examples of the type of money that was being gambled were highlighted during the court cases and include:

- In the evening she would spend between $5,000 and $10,000 on the poker machines, playing two or three machines at a time
- Would regularly use his online account with sports betting organisation Centrebet, where $1.88 million in bets was shown on his Commonwealth Bank credit card
- Had lost about $800,000 at Melbourne’s Crown Casino and more than $200,000 on horse racing and internet gambling
- He punted $48 million
- From 1997 onwards (to 2009), he bet nearly every day
• Internet gambling debt of $17 million
• Said when she was offered inducements by Crown, she started gambling more heavily
• Gambled $8.5 million at Star City. Was on Star City's top 100 turnover list and number three on list of top losers
• Bookmakers flew him to Melbourne business class and was introduced to TV personalities and trainers
• At the peak was putting $40,000 a month into Lotto tickets
• Gambled $6.5 million
• Gambled $1.8 million at Crown Casino from 1997 to 2003
• He lost an average of $1,200 per day gambling
• Transferred the $22.448 million from his employer's bank accounts to the bookmakers. He gambled with Sportingbet, Sportsbet and SA bookies
• He lost $11 million in six months

Lifestyle as a motivator

Lifestyle was the second biggest motivator for million dollar employee fraud.

Some of the types of expenditure incurred by the perpetrators include:
• Travel to the USA, Britain, the Gold Coast, Port Douglas, Hayman Island, Sydney, Melbourne and Thailand, staying in luxury accommodation and spending in designer stores
• Spent on houses, luxury cars, furniture and electrical appliances
• Buying cars, jewellery, a wine collection and luxury travel
• Expensive cars, luxury goods and holidays
• Bought real estate and used money to upgrade the properties with landscaping, refurbishing
• 600 pieces of jewellery from brands including Tiffany, Tag Heuer, Bulgari ($810,000 Bulgari emerald-cut diamond ring and Bulgari necklace with 64 diamonds valued at $556,000) and $16 million with Paspaley Pearls, 200 Chanel products including perfume and make-up, designer clothing from Chanel, Hugo Boss and Armani, 60 pieces of Mont Blanc stationery and a $600 bottle of Moet & Chandon Dom Perignon champagne and hundreds of thousands of dollars worth of Michael Jackson memorabilia including a signed guitar bought from eBay for $US250,000
• Purchased 44 real estate properties, several motor vehicles, jewellery and shares
• Bought cars and caravans and invested $1.5 million into a hotel
• Bought a $3 million house, a yacht and two BMWs
Impact of the frauds on the victims

We have relied on the evidence presented to the courts as to how the frauds impacted on the organisations.

The best way to present the impact on the businesses who suffered the frauds is to list some of the outcomes of the frauds.

These include:

- The theft was one of a number of factors which contributed to the collapse of the business
- The whereabouts of $10 million of the money said to have been fraudulently taken remained unknown
- No impact on client or client funds
- Left bank with debt of $3.2 million
- A significant amount of the missing money ($7 million) has yet to be recovered
- Caused company financial difficulties and traumatised other employees
- Nine account holders were affected
- Write-off to profit could be as high as $30 million
- She and husband had to sell their house to save their company
- The company is still operating at a loss as it tries to recover the rest of the stolen money
- The owner of the panel shop had to sack staff and move to a smaller premises but still debts mounted

The bigger the organisation, the larger the fraud has to be to have a significant impact. Large banks have been able to absorb their frauds with little apparent impact on their operations.

However, the vast majority of the frauds included in this research were publicised by the media. As major companies spend many millions of dollars on their brand, image and values, this type of negative publicity, as a result of a fraud, would be of concern to their board and senior management.

---

**Case Study 7**

**Amount stolen:** $1.1 million  
**Industry sector:** Not-for-profit  
**Motivation:** Lifestyle  
**Sentence:** Three years gaol with a non-parole period of two years  
**Details:** Male, aged 43, defrauded a charity for the homeless to the tune of $1.1 million plus. In his capacity as payroll officer he transferred money into his own personal account over a period of five years. Money was used to support his lifestyle and gambling habit.
Impact of the frauds on the perpetrators

Sentences

Every single person included in this research was sentenced to a gaol term. It is not surprising that Judges and Magistrates refer specifically to the need for a gaol term to act as a deterrent to a breach of trust of such magnitude as a million dollar fraud.

The table below indicates the average length of sentences after taking into account mitigating factors. These are not the head sentences but the minimum terms that the perpetrators faced.

It should be noted that the maximum sentences for frauds will vary between different States and Territories due to sentencing guidelines and precedents.

<table>
<thead>
<tr>
<th>AMOUNT</th>
<th>AVERAGE LENGTH OF GAOL SENTENCE (NON PAROLE PERIOD)</th>
<th>NUMBER OF OFFENDERS</th>
</tr>
</thead>
<tbody>
<tr>
<td>Over $20 million</td>
<td>7 years 4 months</td>
<td>3</td>
</tr>
<tr>
<td>$15 million to $19,999,999</td>
<td>3 years 7 months</td>
<td>4</td>
</tr>
<tr>
<td>$10 million to $14,999,999</td>
<td>4 years 6 months</td>
<td>2</td>
</tr>
<tr>
<td>$5 million to $9,999,999</td>
<td>3 years 8 months</td>
<td>10</td>
</tr>
<tr>
<td>$1 million to $4,999,999</td>
<td>3 years 3 months</td>
<td>74</td>
</tr>
<tr>
<td></td>
<td></td>
<td>93</td>
</tr>
</tbody>
</table>

*Figure 12 – Sentences recorded by size after taking into account mitigating circumstances*

Recompense and financial burden

The repayments at the time of the sentencing may vary from the final recompense. Some perpetrators forego their assets willingly to repay part of the money stolen. Civil action may also lead to further recoveries. Fidelity insurance claims may also result in a reduction in the overall losses.

In addition to the value of the fraud, there are other losses that are directly related and should be taken into account when assessing the true impact. The cost of investigating the frauds, whether by external Forensic Accountants or internally, management time in dealing with the investigation and fallout, legal expenses as well as a possible increase in insurance premiums.

The likelihood of repayment by the perpetrator/s is also diminished by the existence of a gambling problem.
Other impacts

Besides spending time in gaol and repaying some of the funds stolen, those who committed the frauds also had other negative impacts on their lives. These include:

- Attempted suicide afterwards
- Declared bankrupt
- Depression leading to three suicide attempts
- Committed the fraud to support her lover’s drug habit. He was violent towards her. She had not benefitted from the crime
- Estranged from his wife
- Forced to sell home
- Her only asset was a car
- Living in a rented house, drove an old car and had no assets
- Lost his family home to pay back what he stole
- Lost his wife, friends and job
- Now a cleaner. Lost his wife and relationship with his sons
- Suffers from chronic depression
- Wife divorced him
- Wife left him

---

Case Study 8

**Amount stolen:** $10 million plus  
**Industry sector:** Banking  
**Motivation:** Gambling  
**Sentence:** Ten years and six months gaol with a non-parole period of six years  
**Details:** Male, aged 48, held a middle management role for subsidiary of an overseas investment bank. Stole upward of $10 million of company money by falsifying cheques and depositing them into various accounts under the name of his wife. He used the money to support his gambling habit.
Contact us

Warfield & Associates is a professional services firm specialising in Forensic Accounting and the prevention, detection and investigation of unethical behaviour, including fraud and corruption.

As part of our fraud services, we advise organisations on how to mitigate the risk of fraud and corruption from occurring and assist with investigating it when it does occur.

We provide Fraud Awareness Training, undertake Fraud Risk Assessments and Forensic Reviews. We also investigate allegations of fraud and corruption.

For further information about the services offered by Warfield & Associates, please contact us at:

**Warfield & Associates**
Level 57 MLC Centre
19-29 Martin Place
Sydney NSW
Australia

Tel: 612 9231 7588
Fax: 612 9231 7575
E-mail: info@warfield.com.au
Website: www.warfield.com.au