MILLION DOLLAR EMPLOYEE FRAUD IN AUSTRALIA

September 2022

WARFIELD & ASSOCIATES

CONTENTS

INTRODUCTION

Thank you for taking an interest in Warfield & Associates' research into Million Dollar Employee Fraud in Australia. This research study looks at frauds that have been perpetrated by Australian employees where the amount stolen exceeded $1 million Australian and the perpetrator/s have been convicted of that offence in an Australian court of law.

Million dollar plus frauds can have a negative impact on an organisation's customers or clients, as well as its brand, reputation and ultimately bottom line.

Small businesses or not-for-profit organisations may not be able to survive if the amount is large enough to deplete their financial resources. Not-for-profit stakeholders, who provide grants or make donations, may also question their wisdom in choosing that organisation to contribute scarce resources.

This research covers the period August 2012 to August 2022. To be included in the research, the fraud must have satisfied the following criteria:

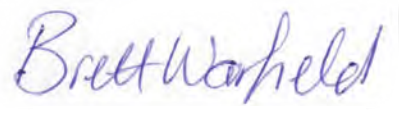
- The amount stolen had to exceed $1 million dollars.
- The fraud resulted in a criminal conviction in an Australian court of law during the above period for an offence that falls under the general umbrella of 'fraud'.
- The fraud had been perpetrated by an employee or employees.

The research focuses on acts of fraud perpetrated by management and staff of organisations, whether they are public or private companies, not-for-profit, associations, government or professional organisations.

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

Being proactive with regards to fraud control is important for all sized organisations.

We hope that this research will assist in helping organisations understand what could happen to them and what they need to do to mitigate the risk as best they can.



Brett Warfield
Principal
Warfield & Associates
September 2022

EXECUTIVE SUMMARY

The key findings of the research include:

- 102 cases were identified involving employee fraud.
- $350 million was stolen.
- 58 of the 102 perpetrators were male and 44 were female.
- Perpetrators ranged in age from 26 to 70 years old.
- Nine perpetrators had prior criminal histories for deception related offences.
- Six cases involved at least $10 million being stolen.
- The largest amount stolen by an employee was $27.4 million.
- The banking and financial services sector was the hardest hit with 15 frauds.
- The longest head sentence delivered was 15 years for a senior finance manager that stole over $20 million in a twelve year period.
- Five of the offenders did not receive a jail term.
- Lifestyle improvement was the main motivating factor in 44 cases.
- Gambling addiction was the main motivating factor in 39 of the cases and a contributing factor in four more.
- False invoicing and electronic funds transfer fraud were the most prevalent ways in which frauds were perpetrated.
- Of the employees who committed fraud against organisations other than banks, 43 were employed in the finance function.
- The shortest time frame for a fraud was four days and the longest was 17 years.
- 52 of the frauds took more than five years to discover.
- Ten cases involved collusion between the perpetrator and either another employee or external party such as a supplier or contractor.

CASE STUDY

Female, aged 50, Data Entry Clerk and Administration Officer. Changed the data on her employer's online banking system so payments intended for internal transfer, or transfer to a third party, flowed to her bank accounts. Two managers that had to enter approval codes in order for the transactions to go ahead, would simply enter their code after checking the total value of the transaction.

Amount Stolen:
$3.79 million

Industry Sector:
Community Housing Provider

Motivation:
Gambling

Sentence:
Five years jail with a non-parole period of two years and six months

ABOUT THIS RESEARCH

Aim of the research

This report presents the findings of a 2022 Australia-wide study into fraud perpetrated by employees. The purpose of this research and our prior fraud research is to increase existing knowledge about the impact of those who betray the trust of their employers. It also aims to guide organisations as to how to reduce the incidence of this type of crime in the future.

Organisations can become more proactive and put in place preventative and detective measures that mitigate the extent and impact of fraud. This can be done by learning from other organisations' mistakes and using that information to assess and address those fraud risks.

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.[1]

The relevant period covered by the research was any conviction in an Australian court of law during the period August 2012 to August 2022, for deception related offences, where evidence was led that the perpetrator was an employee and the amount stolen was in excess of $1 million. The fraud may involve collusion with another staff member or an external party. However, it had to involve employees in the execution of the frauds.

Examples of the types of criminal offences committed that may meet the requirements for inclusion in the research under the general umbrella term of 'fraud' included, but were not limited to:

- Dishonestly dealing with documents.
- 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.

[1] The Australian media landscape is changing and there are less court reporters and therefore less court reports being included in daily newspapers. Also, not all judgements are reported on Austlii and other legal databases. Therefore, it is evident that the research will not be comprehensive in its coverage of all million dollar Australian frauds.

AMOUNTS STOLEN

102 cases totalling $349,996,063 were included in the study. This represented an average of $3.431 million per fraud.

The largest amount stolen was $27.4 million.

Some may think it is quite extraordinary that, in most cases, an employee, most often without the help of other employees, could undertake such deception without being identified by internal controls, management oversight or internal and external audit, for sometimes many years.

Amount Defrauded	Number	Amount
Over $20 million	2	$48,100,000
$15 million to $19,999,999	2	$34,100,000
$10 million to $14,999,999	2	$26,900,000
$5 million to $9,999,999	9	$61,813,239
$1 million to $4,999,999	87	$179,082,824
Total	**102**	**$349,996,063**

Figure 1 – Amounts defrauded by range

CASE STUDY

Female, aged 60, was employed as a Betting Operator for a wagering company for 20 years. In this role she used a glitch in the agency's wagering system to reopen finished races after a false start and put trifecta bets on the victors and collected the winnings through fake accounts. Stole over a period of nine years. Identified when an investigation into suspect betting activities found races were being reopened more often than usual.

Amount Stolen:
$1.42 million

Industry Sector:
Wagering

Motivation:
Gambling

Sentence:
Five years jail with a non-parole period of one year

CASE STUDY

Male, Management Accountant at a metal processor. Set up a shelf company and false invoiced for scrap deliveries over a period of 31 months. Identified by an internal audit. Impacted the perpetrator's job, career and marriage.

Amount Stolen:
$3.1 million

Industry Sector:
Manufacturing

Motivation:
Lifestyle

Sentence:
Six years jail with a non-parole period of four years

THE PERPETRATORS

Sex

Of the 102 frauds 57% of the perpetrators were male.

Sex	Number	Amount	Average
Male	58	$226,945,182	$3,912,848
Female	44	$123,050,881	$2,796,611
Total	**102**	**$349,996,063**	

Figure 2 – Total fraud by sex

The two largest frauds, both exceeding $20 million, were perpetrated by males.

Seven men and three 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 26 and the oldest was 70. The following table breaks down the age groups.

Age Group	Number
60+	12
50 - 59	33
40 - 49	30
30 - 39	24
Under 30	3
Total	**102**

Figure 3 – Fraud by age groups

Role

The perpetrators were identified by a job title and their basic responsibilities. It is not unusual that with a higher level of seniority comes a greater degree of trust.

Staff in Finance and Accounting functions can also be delegated significant responsibility for preparing and approving payments by Electronic Funds Transfers. Cheques are being used far more infrequently now than in our previous survey periods.

Of the employees who committed fraud against organisations other than Banks, 43 were employed in the Finance function.

The most common Finance job titles were as follows:

Job Title	Number
Accountant/Assistant Accountant	8
Accounts Manager/Supervisor	4
Bookkeeper	7
CFO	3
Finance Officer	3
Financial Controller/Manager	4
Payroll Officer	3
Other	11
Total	**43**

Figure 4 – Most common finance job titles

Prior criminal history

Of the 102 perpetrators, nine had prior criminal histories for deception related offences. However, one of those was for fraud offences in New Zealand some 15 years prior. Another offender had an Australian conviction 28 years prior for fraudulent accounting for which she received a suspended three year jail term. Neither of these may have been identified in even the most robust employment screening process. One had a conviction for stealing car radios valued at $3,000 from his previous employer 12 years prior. Another had prior convictions for fraud and armed robbery. A Bookkeeper reoffended in a similar way six months after being released from an 18-month Community Correction Order.

In total, the nine perpetrators were responsible for frauds which totalled $47.078 million.

Background checking / pre-employment screening processes have become far more prevalent in recent years.

Many organisations are requiring criminal record searches be undertaken on some, or all, of their prospective employees. This is likely to have a deterrent effect for prospective employees with prior criminal histories who were considering applying.

Length of employment

Although the length of employment was not stated in each case, the following periods of employment in years were identified:

Range	Number
Under 1 year	1
1 year to under 5 years	7
5 years to under 10 years	13
10 years to under 15 years	9
15 years +	13
Total	**43**

Figure 5 – Length of employment of perpetrators

Was there collusion involved?

The overwhelming number of frauds involved perpetrators acting alone. This is consistent with other fraud research and surveys reporting on employee fraud.

However, there were ten cases of collusion in the study.

Of the ten cases, eight involved false invoicing.

One involved collusion with a fellow staff member to create and approve false transport documentation. Another included three co-accused employees as well as a number of contractors who issued false invoices. A third involved a senior staff member in a bank colluding with a provider of HR resources to false invoice the bank for services not performed.

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. Examples of this included transferring company funds into the bank account of a fellow employee who then transferred it on.

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. In these circumstances, they were not regarding as actively colluding.

HOW WERE THE FRAUDS COMMITTED?

Method	Number	Amount	Average
EFT to own benefit/account	38	$88,709,306	$2,334,455
False invoicing	26	$152,693,577	$5,872,830
Multiple frauds used	11	$18,114,426	$1,646,766
Other	5	$10,981,719	$2,196,344
Trust fraud	5	$12,989,020	$2,597,804
Fraudulent loans	4	$12,517,190	$3,129,298
Cheque fraud	3	$6,734,623	$2,244,874
Stole from customers' bank accounts	3	$14,091,862	$4,697,287
Leasing/Finance fraud	3	$6,789,845	$2,263,282
Cash theft	2	$5,674,495	$2,837,248
False accounting	2	$20,700,000	$10,350,000
Total	**102**	**$349,996,063**	

Figure 6 – Methods of fraud

EFT fraud

In 38 cases the perpetrators transferred some or all of the fraudulently obtained funds into their own bank accounts via the Electronic Funds Transfer (EFT) system.

Examples of the ease with which some did this is evident in the following information:

- 215 occasions involving unauthorised transfers of moneys to the employee's personal bank account over five years.
- Processed a string of payments into bank accounts she and her parents controlled, while sending duplicate amounts to customers to cover the crime.
- 363 direct transfers to himself.
- Masked 52 transactions as payments to the tax office but paid to herself instead.
- 51 transfers to own bank account.
- Transfers into bank accounts in both his name and his parents' names.
- 93 transfers to own bank account and 303 payments to her own Mastercard.
- Transferred money on 866 occasions into her own bank account.
- 107 transfers made to own bank account.
- 70 transfers to own bank account.
- 236 payments to herself into seven separate bank accounts at three banks.
- 1,478 transfers to herself over six years from the business's NAB bank accounts.

The predominant use of EFTs by businesses to pay creditors and staff has placed greater responsibility in the hands of staff. Also, with the recent impact of COVID-19 there has been more decentralisation of the workforce. This has included staff who use their computers at home to transfer significant sums of money on behalf of their employer. Unless there are adequate controls over the EFTs, this type of fraud will continue in the future. We believe that if one lesson is learnt from this research it is that organisations must ensure the controls over their EFTs are regularly reviewed by those with a good understanding of how the systems can be manipulated.

False invoicing

False invoicing continues to be one of the most prevalent methods of fraud. Invoices are created for goods or services that have either never been rendered, or for which the fees have been greatly exaggerated. Examples included:

- Faked proof of delivery dockets which he used to justify payments to his own companies, unbeknown to their employer.
- Set up two companies which issued more than 700 invoices to his employer for which no produce was ever supplied. One of the methods used to cover his tracks was by adjusting the weight of stock already in the system from other suppliers.
- 299 false invoices issued by a false supplier over 12 years.
- 400 fraudulent invoices over two and a half years.
- Raised hundreds of invoices for non-existing services over 13 years.
- 50 purchase orders for IT hardware of which only one was delivered.
- 337 altered invoices.

CASE STUDY

Male, aged 51, working as a Credit Collection Officer, defrauded the transport company in collusion with a friend and co-worker. They set up sub-contracting companies and arranged false invoices to be paid to the company by their employer based on their approval of false proof of delivery dockets.

Amount Stolen:
$3.488 million

Industry Sector:
Transport

Motivation:
Gambling

Sentence:
Five years jail with a non-parole period of two years and six months

FRAUD BY INDUSTRY

The financial services sector was hit heavily by frauds in the research period. Ten were banks and five were other financial services related organisations.

Industry	Number	Amount
Construction	11	$36,876,765
Banks	10	$39,574,148
Manufacturing	9	$24,218,972
Not-for-profit	6	$11,437,162
Real Estate and Property	6	$13,698,231
Other Financial Services Institutions	5	$8,479,935
Retail	5	$11,989,536
Transport	5	$10,069,215
Advertising and Media	4	$13,870,578
Government	4	$46,238,879
Hospitality	4	$13,386,383
IT/Technology	3	$12,419,893
Legal Firms	3	$6,034,836
Aged Care	2	$4,100,000
Construction Materials	2	$15,131,719
Education	2	$9,108,777
Insurance	2	$18,400,000
Medical	2	$3,511,632
Mining	2	$5,300,000
Motor Vehicle Dealers	2	$3,000,098
Other	13	$43,149,304
Total	**102**	**$349,996,063**

Figure 7 – Frauds by industry

CASE STUDY

Female, aged 48, Payroll Officer. On 220 occasions, over a six year period, transferred amounts from her employer's bank account to various accounts related to her. She created fraudulent documentation for every one of the unauthorised transactions and used false names. Used the money to buy a Pie Face franchise, invest in properties, payments to relatives and entertaining friends and relatives at social and sporting events. She had committed two acts of fraud at previous employers and had previously been incarcerated.

Amount Stolen:
$4.142 million

Industry Sector:
Packaging

Motivation:
Lifestyle

Sentence:
Six years and four months jail with a non-parole period of four years

DURATION OF FRAUDS

The longest period a fraud went undetected was for 17 years, involving $3.7 million being stolen from a manufacturing company specialising in paints.

One fraud was committed over just four days.

The duration of time taken to discover frauds should be of 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 extraordinary period of time.

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.

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?

Duration of Frauds	Number	Amount	Average
10 years +	13	$86,879,944	$6,683,073
5 years up to less than 10 years	39	$118,246,567	$3,031,963
3 years up to less than 5 years	15	$57,053,488	$3,803,566
2 years up to less than 3 years	14	$48,219,205	$3,444,229
12 months up to less than 2 years	10	$23,398,468	$2,339,847
6 months up to less than 12 months	4	$7,495,371	$1,873,843
Less than 6 months	7	$8,703,020	$1,243,289
Total	**102**	**$349,996,063**	

Figure 8 – Time taken for fraud to be discovered

CASE STUDY

Female, aged 59, working as a Finance Officer. Made 27 transfers from the club's bank account to overseas accounts. Subject of a romance scam. Lost her own money then stole from the club.

Amount Stolen:
$1.1 million

Industry Sector:
Sports Club

Motivation:
Romance Scam

Sentence:
Three year intensive correctional order

HOW WERE THE FRAUDS DISCOVERED?

In approximately two thirds of the cases, the way the frauds were discovered was disclosed. Though in some cases it was not specific, merely stating it was 'discovered internally' or 'internal controls'.

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 a number of 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. This is called fraud awareness training.

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:

- Investigation commenced when irregular bank transactions were discovered.
- Bank suggested owner review his finances.
- Bank notified the company of irregularities.
- Blank cheque butts discovered by a senior manager were raised with the Office Manager, who subsequently left and never returned to work.
- Poor cash flow resulted in Bookkeeper being engaged, who subsequently discovered the fraud.
- Contractors complained their invoices had not been paid.
- Whilst the perpetrator was on holidays.
- Profitability concerns led to an auditor being hired to conduct a review.
- Investigation into suspect betting activities.
- Review of an 'unusual' monthly stocktake report identified two suppliers that were not recognised.
- New CFO began asking questions and alerted the audit committee who brought in investigators.
- General Manager of the Australian operations of the company identified what was described as a bonus which proved to be unauthorised.
- Consumer Affairs investigation.
- Internal review of expenditure.
- Branch Manager noticed the ATM balances were unusually high.
- Suspicious relationship with a supplier revealed in emails.
- Creditors contacted a Director stating they had not been paid.
- When the firm implemented a new EFT safeguard.
- Financier was engaged to audit their accounts, review company processes and make recommendations for improvement.
- Subcontractor approached the Chief Operating Officer at a function asking about additional contract work. This contrasted to the amount of work they were already being paid for. The COO then commenced an investigation.
- Expenditure on hospitality was not approved and led to an investigation.
- Creditors contacting the organisation chasing payments.
- Complaint made to the CEO's office.
- New Finance Manager, who took over from the perpetrator after they had resigned, discovered unusual payments.
- Member of a superannuation fund complained about their account. Staff member then wrote a letter to his employer admitting to the fraud.
- Senior Manager found anomalies in the financial accounts.
- Perpetrator made admissions to the owner during a due diligence visit by prospective buyers of the business.

INTERNAL CONTROL BREACHES

Examples of how internal controls were breached included:

- Used colleagues' personal details and forged signatures on bank cheques to approve the loans.
- Took advantage of company's accounting system which was in disarray during a system change-over.
- Doctored the holdings of the branch, then electronically transferred the money to an ATM and entered false balance sheets before stealing the cash.
- Lack of segregation of duties allowed one person to count the cash takings, prepare the deposit slip and undertake the physical banking of cash.
- Lack of review and oversight of creating new creditors allowed 1,500 payments to be paid to fake creditors.
- Copied and pasted the signature of two board members onto an approval document.
- Lack of segregation of duties in changing creditor bank account details.
- Expenditure identified as being outside the staff member's delegated authority.
- Reversing receipts for payments put the accounts temporarily into a negative balance. However there was no reporting trigger to notify customers or management within the financial institution of this occurrence.
- Either misled a colleague into signing cheques, or issued them himself without a co-signature.

CASE STUDY

Male, aged 58, worked as a Financial Controller of a secondary school. Fraud perpetrated over a 15 year period. Changed details in the school's tax portal to redirect 39 GST refunds totaling $3.993 million into his own bank account. Also made 363 transfers to his own bank accounts. Discovered by the new Financial Controller after the perpetrator had left the school.

Amount Stolen:
$7.409 million

Industry Sector:
Secondary Education

Motivation:
Gambling

Sentence:
Nine years jail with a non-parole period of five and a half years

WHAT WAS THE MOTIVATION?

Often in fraud cases there is clear evidence of asset accumulation, lifestyle choices or a gambling addiction.

Based on evidence provided to the courts, we have endeavoured to identify the motivation in each case. Lifestyle improvement and gambling were the main reasons the frauds were committed.

Even when assessing some frauds that appear to be motivated by lifestyle, there were clear indications of more deep seated emotional and psychological issues that resulted in the perpetrator's irrational behaviour. This has been a trend in previous research undertaken by Warfield & Associates.

Motivating Factors	Number	Amount	Average
Improve lifestyle	44	$198,860,639	$4,519,560
Gambling	39	$90,118,445	$2,310,729
Multiple factors	8	$27,219,095	$3,402,387
No explanation	3	$14,551,323	$4,850,441
Prop up failing businesses	2	$4,699,020	$2,349,510
Romance scam	2	$2,612,705	$1,306,353
Personal financial pressures	2	$5,900,000	$2,950,000
Drugs	1	$2,034,836	$2,034,836
Altruism	1	$4,000,000	$4,000,000
Total	**102**	**$349,996,063**	

Figure 9 – Motivating factors for the frauds

CASE STUDY

Male, aged 37, worked as a CFO of a Shire Council. Over a two month period intentionally overpaid 14 contractors and suppliers and requested they transfer the money back to his own bank account, unbeknown to the contractors and suppliers. Discovered when a staff member identified an irregular bank transfer.

Amount Stolen:
$1.039 million

Industry Sector:
Local Government

Motivation:
Unknown

Sentence:
Five years jail with a non-parole period of two years

Lifestyle as a motivator

Lifestyle was the biggest motivator for million dollar fraud. There were 44 cases where this was the main motivating factor.

Some of the types of expenditure incurred by the perpetrators include:

- Over $400,000 on jewellery, $220,000 on clothes, $400,000 on household expenses and over $50,000 on duty-free goods and department store spending. Also mortgage repayments and travel.
- Bought an Aston Martin car, spent tens of thousands of dollars on travel, dining and jewellery and his wedding at a Canberra hotel. Also purchased a doll house worth $10,000 and paid off a house in Adelaide.
- Family holidays, cars, jewellery, tattoo studios and baby stores.
- Two Porsches for $280,000 and gifted one to his girlfriend. $300,000 on 26 designer watches. Deposit on his sister's apartment. Mortgage repayments on his ex-wife's home.
- Repay a $10 million mortgage.
- $109,000 deposit on a house.
- $366,993 on holiday trips between 2011 and 2019.
- $58,000 on cosmetic surgery.
- Bought a car, holidays to Fiji and Queensland, jewellery and other gifts, supported her family, funded her then boyfriend's failed career as a rap musician and paid for his legal fees.
- Bought a cafe with more than $600,000 of the stolen funds.
- Paid off her and her husband's business and personal debts and purchased two new cars.
- Expensive holidays, cars, motorbikes, property and funding a drag racing business over several years.
- BMW, hotels, trips, and Star Wars memorabilia.
- $41,875 on luxury goods, $134,073 on strip clubs and $65,944 on travel.
- Three 'special interest military vehicles' bought for her husband.
- Purchased expensive properties in his own name and wife's name and bought interests in 111 horses totalling $7 million.
- Lunches, wine, cocaine, girls and buying a house where he lived with his new bride. Also paid off a loan over a business deal that went bad.
- Spent $250,000 on travel and accommodation.
- Real estate, home renovations, vehicles, additional superannuation contributions, shares and holidays.
- $1.1 million on travel and accommodation, $140,000 on clothes, $6.2 million on property, $637,000 with Louis Vuitton.

Gambling as a motivator

39 of the 102 perpetrators of fraud in this research had a gambling addiction as the main motivating factor. Another four cases had gambling as one of the main factors in contributing to the frauds. These are included in the multiple factors section of the above table.

Further analysis was undertaken of the modes of gambling in order to understand what forms of gambling were most attractive to the perpetrators.

Preferred gambling modes were not always identified. Also, 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.

Mode of Gambling	Number	$	Average
Poker machines	12	$33,785,139	$2,815,428
Casinos [2]	5	$7,371,324	$1,474,265
Horseracing	2	$2,646,383	$1,323,192
Internet Sports Gambling	5	$20,623,581	$4,124,716
Other (Tattslotto, TAB, and multiples of any of the above modes) [3]	6	$11,244,828	$1,874,138
Unknown	9	$14,447,189	$1,605,243
Total	**39**	**$90,118,444**	

Figure 10 – Main types of gambling that the fraud proceeds were used for

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

- In one day, he lost $190,000 on a soccer game, won $278,000, lost the winnings on another game, then bet another $120,000 and won $387,000, which he bet once more to walk away with $774,000.
- Ploughed almost $1.5 million of the money she stole into poker machines at Crown Casino.
- Saw him spend up to 16 hours at a time on slot machines at casinos in Perth and Melbourne where he was given high roller status.
- Spent about $2,500 a week on poker machines.
- Within 12 months was gambling daily on poker machines and Tattslotto.
- Would place up to 100 bets a day in a variety of ways including online and through a mobile phone application and would bet on a range of sporting events including during football games.
- Poker machine habit averaged $500 in losses every day for seven years.
- Gambled more than $30 million at the Reef Hotel Casino on poker machines over six years. This resulted in $2.9 million of embezzled money being lost at the Reef Hotel Casino.
- Spent up to $15,000 per week at the TAB or Crown Casino.
- Betting more than $3.5 million over two years.
- Had a 25 year gambling addiction.
- Records from Crown Casino indicated she lost about $1.2 million gambling over a four year period.
- Gambled $10 million in one leagues club alone over six years.

[2] This excludes references to poker machines played at a casino, which have been included in the poker machine figures.
[3] This includes four further instances where poker machines were one of the modes of gambling.

IMPACT OF THE FRAUDS ON THE VICTIMS

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

The impacts on the businesses who suffered the frauds included:

- Business was liquidated.
- Company had to downsize and sell assets.
- Seven stores closed and 60 staff lost their jobs.
- Liquidation of the agency.
- Liquidation of the company.
- 16 staff lost their jobs.
- Difficulty in obtaining insurance and lost business opportunities.
- Stress on the owners and staff.
- Not only lost $1.7 million but had to then pay the $1.7 million owing to the ATO that had been diverted.
- Went into Administration and was in the process of liquidation as at the sentencing date.
- Business owner had to take out a $1 million mortgage to cover the stolen funds.

The larger the organisation, the bigger the fraud has to be to have a significant impact. Large organisations 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 Boards and Senior Management.

CASE STUDY

Male, Finance and Administration Manager in his 50s, created 300 false invoices and made payments to his own business bank account. Misappropriated money over a 12 year period. Had worked for the company for 30 years. Money was spent on expensive thoroughbred horses, at least six properties and a lover. A lack of segregation of duties contributed to the fraud being undetected for so long.

Amount Stolen:
$20.7 million

Industry Sector:
Construction

Motivation:
Lifestyle

Sentence:
Fifteen years jail with a non-parole period of five years (on appeal)

IMPACT OF THE FRAUDS ON THE PERPETRATORS

Sentences

Judges and Magistrates refer specifically to the need for a jail term to act as a deterrent to a breach of trust of such magnitude as a million dollar fraud. However, five offenders did not receive a jail sentence. Instead, they received an Intensive Corrections Order from the court.

The longest head sentence delivered was 15 years for a senior finance manager that stole over $20 million in a twelve year period. The non-parole period was initially set at six years, but was reduced to five years on appeal.

The longest non-parole period delivered was ten years. It involved collusion between employees in a government department over more than 11 years that resulted in the loss of more than $20 million. 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.[4]

The maximum sentences for frauds will vary between different States and Territories due to sentencing guidelines and precedents.

Amount	Average Length of Jail Sentence (non-parole period)	Number of Offenders
Over $20 million	7 years 6 months	2
$15 million to $19,999,999	6 years	2
$10 million to $14,999,999	6 years	2
$5 million to $9,999,999	4 years 4 months	9
$1 million to $4,999,999	2 years 9 months	87
Total		**102**

Figure 11 – Sentences recorded by size after taking into account mitigating circumstances

[4] These are averages and should not be used to indicate the likely sentence a person may receive in the event that they are convicted as there are a range of factors taken into account by Judges and Magistrates when sentencing those who have been convicted.

Recompense and financial burden

The repayments made to employers 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 through freezing orders. Fidelity insurance claims may also result in a reduction in the overall losses.

The cost of investigating the fraud may include external Forensic Accountants or investigators' fees, management and employee 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 was also diminished by the existence of a severe gambling problem, as most of the fraudulently obtained funds were used to gamble. Those with a gambling addiction also used their own assets to gamble and this resulted in a lack of resources to repay their employer.

Several of the organisations were fortunate that they were reimbursed all of the money stolen. However, this was the exception and not the rule.

Other impacts

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

- Bankruptcy.
- Living with parents.
- Marriage break down.
- Selling the family home.
- Struck off the legal register.
- Borrowing from their family to repay stolen funds.
- No residual assets.
- Husband found guilty of six counts of money laundering and jailed as well.
- Nothing left in her superannuation account.
- Suicide.

JUDGES' AND MAGISTRATES' COMMENTS

"Your conduct has caused enormous damage to that company. It may result in the company going into liquidation". Judge Helen Bowskill, Southport District Court.

"Your offending has had significant consequences. The company was initially placed in administration but is currently in liquidation. I am satisfied that the theft of such a significant amount of money from the company has been a cause of the company's demise". Judge Irene Lawson, County Court of Victoria.

"You were driven by an insatiable need to look successful and appear to be wealthy". Judge Frances Hogan, County Court of Victoria.

"Wholly unjustified sense of entitlement". Justice Christine Adamson, NSW Supreme Court.

"He said he decided to do this as he had a fairly severe gambling problem and was always trying to find money to fund the gambling. He found a loophole, and took advantage of it". Judge Karen Robinson, NSW District Court.

"This was a fraud of massive proportions. It took considerable planning and skill to pull this off and what's more to avoid detection for nearly 10 years. Even though you were caught red handed you have not displayed any remorse whatsoever". Judge Brian Harrison, Cairns District Court.

"Your fraud was discovered because your ex-husband noticed some anomalies in a shared account and told the relevant interested parties". Judge Tony Moynihan, Mackay District Court.

"When you became aware that an internal audit or inquiry was being made, you began to perhaps cover your tracks by concealing some of the transfers". Deputy Chief Magistrate Jane Culver, Downing Centre Local Court.

"In addition I accept that you have re-ordered your life and that since the police became involved you have been living with the anxiety of not knowing whether you would be the subject of an immediate term of imprisonment". Judge Gavan Meredith, County Court of Victoria.

"Unfortunately, under pressure, you made extremely irresponsible business decisions". Judge Carolyn Douglas, County Court of Victoria.

CONTACT US

WARFIELD & ASSOCIATES

Warfield & Associates is a professional services firm specialising in corporate investigations, forensic accounting, the prevention, detection and investigation of unethical behaviour, including fraud, bribery and corruption.

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

We provide fraud and corruption awareness training, undertake fraud and corruption risk assessments and forensic reviews.

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

Warfield & Associates
Level 21
133 Castlereagh Street
Sydney NSW 2000
Australia

Tel: 02 8005 3005
E-mail: info@warfield.com.au
Website: www.warfield.com.au