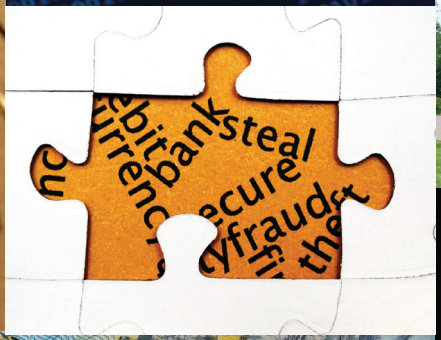

Employee Fraud in Australian Financial Institutions

Author : Brett Warfield, Partner, Warfield & Associates

WARFIELD
& ASSOCIATES

Contents

Foreword 3
Executive summary 4
About this research 5
Aim of the research 5
How the research was undertaken 5
About the author 6
Amounts stolen 7
The perpetrators 8
Sex 8
Age 9
Role 9
Prior criminal history 9
Was there collusion involved? 10
How long were they employees when they stole? 10
How were the frauds committed? 11
Where were the frauds perpetrated? 13
Duration of frauds 14
How were the frauds discovered? 15
Warning signs that were ignored 17
What was the motivation? 17
Gambling as a motivator 18
Lifestyle as a motivator 20
Impact of the frauds on the employers 21
Impact of the frauds on the perpetrators 22
Sentences 22
Recompense and financial burden 22
Other impacts 23
Contact us 24

Foreword

When financial institutions have a fraud, one of their first concerns is 'did it affect our customers?'. In 2013, financial institutions face a myriad of external threats from cyber hacking, mortgage loan fraud, credit card fraud, money laundering, ATM fraud, cheque fraud and identity theft. They also face the enemy within.

The fact that one of their staff was involved increases the likelihood that customers' funds have been misused. Many frontline and back office staff have access to customer information and accounts. Staff require access to databases of information to do their job.

The question is 'How does their employer ensure they use this information and access for the benefit of their employer and their customers and clients and not for their own self interest?'.

This and other questions were put to a number of industry professionals who assisted with their views about internal fraud. Their opinions have been greatly appreciated and have added some insight to the statistics in this report.

This research looks at frauds in recent history in Australia that have been perpetrated by employees of financial institutions. It is a sample of the cases that have come to light in a public forum. It is not representative of all cases that have occurred within financial institutions.

It should also be emphasised that the financial institutions in Australia employ hundreds of thousands of staff who are honest, diligent, hard working contributors to the success of their organisations. The small minority have been highlighted in this research.

The research focuses exclusively on acts of fraud committed by management and staff of organisations which as part of their structure accept deposit funds at a retail level. It covers the period 1 January 2000 to 30 September 2013.

To be included in the research, a fraud must have satisfied the following criteria:

- 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, or which involved an employee, even though an outside party was also complicit.

Employee Fraud in Australian Financial Institutions is the fifth major fraud research study undertaken by Warfield & Associates since 2008.

We trust this new research can assist organisations to learn from the mistakes of others and minimise the risk of fraud on their brand, reputation and bottom line.

Brett Warfield
Partner
Warfield & Associates
November 2013

Executive summary

The key findings of the research include:

- $217,266,481 was stolen.
- Five cases involved at least $10 million.
- The largest amount stolen by an employee was $45.3 million.
- 120 cases were identified involving 123 employees.
- 69 of the cases involved one of the 'Big 4' banks.
- 68 of the perpetrators were male and 55 were female.
- Perpetrators ranged in age from 20 to 60 years old.
- At least 30 of the perpetrators had been employees for ten years or more before they stole.
- At least five perpetrators had prior criminal histories for deception related offences.
- One of the perpetrators had three prior convictions for gambling related frauds and yet no detailed background check was undertaken on him. He went on to steal just under $1.2 million.
- 92% of the cases involved a perpetrator acting alone.
- 104 of the 123 offenders served time in gaol.
- Gambling addiction was the main motivating factor in 62 of the cases. This makes up more than half the cases in the research.
- The most common ways staff stole was to either steal from customers' bank accounts or term deposits or else create false loans.
- On at least 20 occasions the customers notified the financial institution of the fraud on their accounts.
- Victoria had the most number of frauds yet NSW incurred the biggest losses totaling $115 million, which is more than half the national total.
- One in six of the frauds took more than five years to discover.
- The duration of time taken to discover frauds should be of real concern to those responsible for governance in their financial institutions.
- It is clear that educating staff about the warning signs of fraud and fraud risk mitigation strategies have been absent in many of the reported cases.

About this research

Aim of the research

This report presents the findings of a 2013 Australia-wide study into fraud perpetrated by employees of financial institutions.

The aim of this research is to obtain factual information about actual cases of employee fraud to determine if there were any patterns of behaviour or lessons that can be learnt. The past is often a good guide as to what may happen in the future.

How the research was undertaken

The research involved an extensive review of online law judgements, as well as Australian newspaper articles containing court reports that provided details of judgements. Therefore, all cases had to have been made public.

The relevant period covered by the research was any conviction in an Australian court of law during the period 1 January 2000 to 30 September 2013, for deception related offences, where evidence was led that the perpetrator was an employee of a financial institution.

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

- Dishonestly manipulating machine for benefit
- Dishonestly taking property without the owner's consent
- Embezzlement
- False accounting
- Falsification of accounts
- Forgery
- Fraud
- Fraudulent misappropriation
- Larceny by a clerk
- Make false document
- Make false instrument
- Making false entries
- Misappropriation
- Obtain property by deception
- Obtaining financial advantage by deception
- Stealing as a servant
- Theft
- Use false document
- Uttering

About the author

Brett Warfield is a Sydney based Forensic Accountant and Partner of Warfield & Associates.

Warfield & Associates specialises in governance and the prevention, detection and investigation of unethical behaviour, including fraud and corruption. It works with clients to mitigate risk and protect their brand, reputation and bottom line.

Brett has twenty-five years experience including seven years in senior management with KPMG Forensic in Australia. Prior to KPMG he had nine years as a Financial Investigator with four of Australia's leading corruption investigation bodies including the Royal Commission into Productivity in the Building Industry in NSW and the Wood Royal Commission into the NSW Police Service, the NSW Building Industry Task Force and the Independent Commission Against Corruption. Prior to that he was a financial and management accountant with BHP Co Ltd.

He has been a frequent commentator on topical public issues over the years on ABC Radio and Television, SBS Television and quoted in articles in the Australian, Sydney Morning Herald, the Age, Australian Financial Review, Courier Mail, Daily Telegraph, Sunday Telegraph, Herald Sun, CFO, Business Review Weekly, Charter Magazine, SmartCompany and Choice Magazine.

He regularly presents at conferences and seminars.

Brett is a member of the Governance Institute of Australia and has the following professional qualifications:

- Bachelor of Commerce, University of New South Wales
- Graduate Diploma in Applied Finance and Investment, Securities Institute of Australia
- Master of Business Administration (Exec), AGSM
- Graduate Certificate in Fraud Investigation, Latrobe University
- Graduate Diploma in Applied Corporate Governance, Chartered Secretaries Australia

Amounts stolen

120 cases were included in the research involving the theft of $217,266,481. This represented an average of $1.811 million per fraud.

There were 33 cases that exceeded $1 million.

Large financial institutions can withstand a large fraud. 69 of the cases involved one of the 'Big 4' banks. 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 financial institutions, the impact can be far greater.

Regardless of an organisation's size, a fraud exceeding $10 million would hurt its reputation, the Board's confidence in its senior management and stakeholders' confidence that there is adequate governance over the management of the business.

AMOUNT DEFRAUDED	NUMBER	AMOUNT
Over $10 million	5	$100,932,881
$5 million to $9,999,999	7	$49,373,004
$1 million to $4,999,999	21	$42,755,565
$100,000 to $999,999	58	$22,984,560
$50,000 to $99,999	12	$841,887
Up to $49,999	17	$378,584
Totals	**120**	**$217,266,481**

Figure 1 – Amounts defrauded by range

The perpetrators

The first question to be asked is 'what is an employee?'.

Today, many organisations have contractors who take on the role of an employee in all but name. Some are agents for the financial institutions and are held out to the public as representatives of those institutions even though they are employed by another organisation who has the licence. They are given the responsibility of taking customers' deposits and being involved in organising investments and loans.

Similarly the mortgage broking business model has changed in the past couple of decades. Mortgage brokers can sell a range of different financial institutions' products or can be aligned with one financial institution exclusively. It is with this exclusivity where the branding of the brokers or agents could lead to them being classed as 'employees'.

Financial planners can work exclusively with one financial institution or sell the products of any institution for which they are approved.

They could all be mistaken as employees by investors and there may be an argument for ensuring they undergo all pre-employment screening processes and training and education on conduct and ethics that employees are subject to, as there can be significant reputational risk of having an agent, broker or planner go 'rogue'.

However, for the purpose of this research, a very strict definition has been used. That is, that the person must be employed by the financial institution and not be an agent or broker regardless of their exclusivity.

Sex

There were 123 perpetrators involved in the 120 frauds included in the research.

55% of the offenders were male.

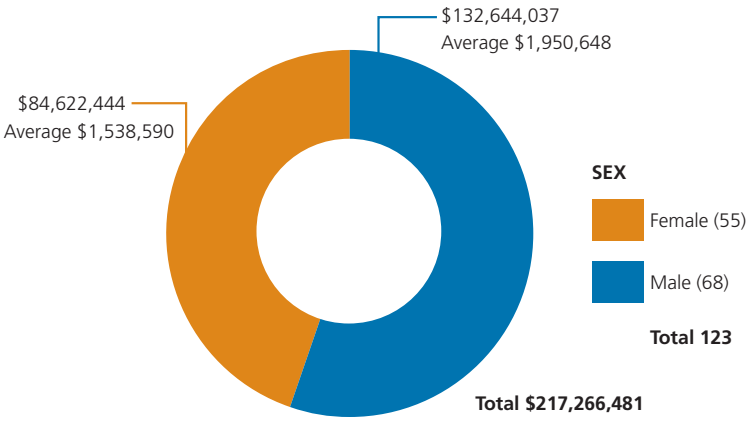

Figure 2 – Total fraud by sex

The largest single fraud in the study of just over $45.3 million was perpetrated by a woman.

Males were responsible for seven of 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 20 years old and the oldest was 60.

Where there were two perpetrators involved, the amount stolen was averaged between the two age groups. The following table breaks down the age groups.

AGE GROUP	NUMBER	AMOUNT	AVERAGE
20-29	23	$15,434,141	$671,050
30-39	51	$75,465,725	$1,479,720
40-49	39	$113,676,203	$2,914,774
50-59	9	$11,864,412	$1,318,268
60 +	1	$826,000	$826,000
	123	**$217,266,481**	

Figure 3 – Fraud by age group

Role

The perpetrators were identified by a job title and their basic responsibilities. In some cases this appeared to be a generic title that could mean different things in different organisations. The titles were many and varied and included Accountant, Assistant Vice President Implementation, Cash Settlements Officer, Client Services Manager, Corporate Accounts Manager, Financial Adviser, Financial Services Administrator, Manager Equipment Finance, Relationship Manager, Securities Dealer, Senior Fraud Investigator, Senior Manager Treasury and Trade Relationship Officer.

The three most common job titles were Tellers, Branch Managers and Loans/Lending Manager/ Officer.

Prior criminal history

Of the 123 perpetrators in the 120 cases, five had prior criminal histories for deception related offences. In total, the five perpetrators were responsible for frauds which totalled $2.7 million.

One of the perpetrators had three prior convictions for gambling related frauds and yet no detailed background check was undertaken on him. He went on to steal just under $1.2 million.

One other perpetrator had previously been convicted of murder. He went on to commit a fraud of over $1.2 million.

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. These can also act as a deterrent to potential fraudsters and therefore their true value can be difficult to gauge. It would be foolish, but not unknown, for a person with a criminal history to apply for employment and not disclose it as relevant to their prospective employment.

Was there collusion involved?

Four cases had at least two staff members colluding to commit the frauds. In each case the amount stolen exceeded $500,000.

On another six occasions, staff were assisted by external parties such as customers, associates or criminal syndicates to perpetrate the frauds. Four of these exceeded $1 million.

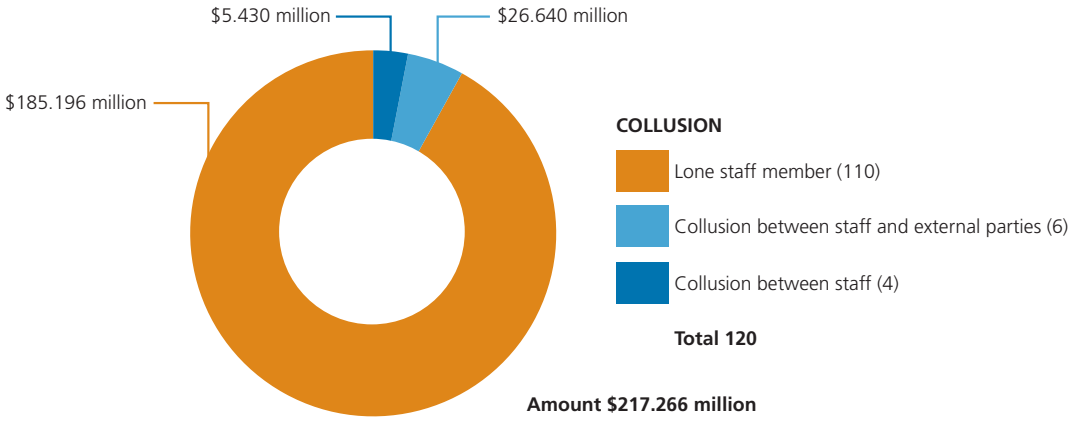

Figure 4 – Was collusion present?

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 knowingly or unknowingly.

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. Where this was unknowing, they were not regarded as actively colluding.

The fact that 92% of the perpetrators of the frauds acted alone is consistent with other fraud research and surveys reporting on internal fraud.

How long were they employees when they stole?

Of the 123 offenders, their length of employment prior to committing the frauds was identified on 46 occasions.

30 of the 46 perpetrators were employees for at least ten years prior to offending. Why do employees of such long standing commit fraud against their employer? Further research into this area would be enlightening.

EMPLOYMENT LENGTH	NUMBER	AMOUNT	AVERAGE
< 3 months	2	$1,094,617	$547,309
3 months to < 6 months	2	$193,700	$96,850
6 months to < 2 years	2	$165,324	$82,662
2 to < 5 years	5	$1,031,563	$206,313
5 to <10 years	5	$21,967,055	$4,393,411
10 to < 20 years	15	$24,351,921	$1,623,461
> 20 years	15	$75,473,230	$5,031.549
	46	**$124,277,410**	

Figure 5 – Length of employment of perpetrators

How were the frauds committed?

In 41 cases the perpetrators transferred some, or all, of the fraudulently obtained funds directly from customers' bank accounts and term deposits.

Fraudulent loans was the second most popular way staff stole and was done by either creating false names and addresses or establishing loans in the names of existing customers without their knowledge.

METHOD	NUMBER	AMOUNT	AVERAGE
Stole from customers' bank accounts and term deposits	41	$50,033,378	$1,220,326
Fraudulent loans	27	$40,615,410	$1,504,274
Other one-off frauds	10	$4,170,005	$417,001
Stole from ledger, suspense or general accounts (non customer related)	9	$21,943,042	$2,438,116
Theft of cash from ATM, safe or cash drawers	6	$1,635,540	$272,590
Multiple frauds	6	$14,567,500	$2,427,917
EFT to own bank account and other related third parties	5	$65,774,652	$13,154,930
Fraudulent credit cards	5	$2,375,489	$475,098
Unknown	5	$2,190,478	$438,096
Cheque fraud / Stolen cheques	4	$11,264,411	$2,816,103
False invoicing	2	$2,696,576	$1,348,288
	120	**$217,266,481**	

Figure 6 – Method of fraud

Examples of how the fraud were done included:

- Altered records relating to term deposits held by 6 elderly customers to cover withdrawals
- Arranged loans without customer's knowledge
- Conducted 141 unauthorised transactions from the accounts of 21 customers over a 10-month period
- Created fictitious loan in mother's name. Created another 6 fictitious loans. Then another 9 accounts
- Established 20 false loan accounts
- Established 54 fraudulent loans for fictitious borrowers, with names either made up or plucked from the telephone book
- Forged 76 cheques over 5 years
- Created 33 false accounts
- Shifted money from a suspense account to a foreign currency account
- Inflated 49 invoices for construction work
- Made 17 loan applications of which 15 were approved and paid into her accounts
- Made 22 transfers to his own bank account
- On 89 occasions he moved money between accounts
- Performed 101 fraudulent transactions over a 14 month period
- Shifted $22 million between accounts over four years to hide her thefts
- Stole on 879 occasions
- Stole from an 85 year old pensioner's account
- Stole money from a dead woman's account
- Stole the money through the Branch Telling Service by transferring an average of $1,000 from a general ledger account, used to pay property valuers, into accounts of her own
- Submitted 42 false commission invoices over 1.5 years
- Unlawfully withdrew funds from a general ledger a/c and deposited them into her own account
- Went on to assume the identities of other customers using 87 credit cards

Where were the frauds perpetrated?

The frauds were broken down by the State and Territory in which they occurred.

Victoria had the most frauds by number, however NSW had the greater value of losses.

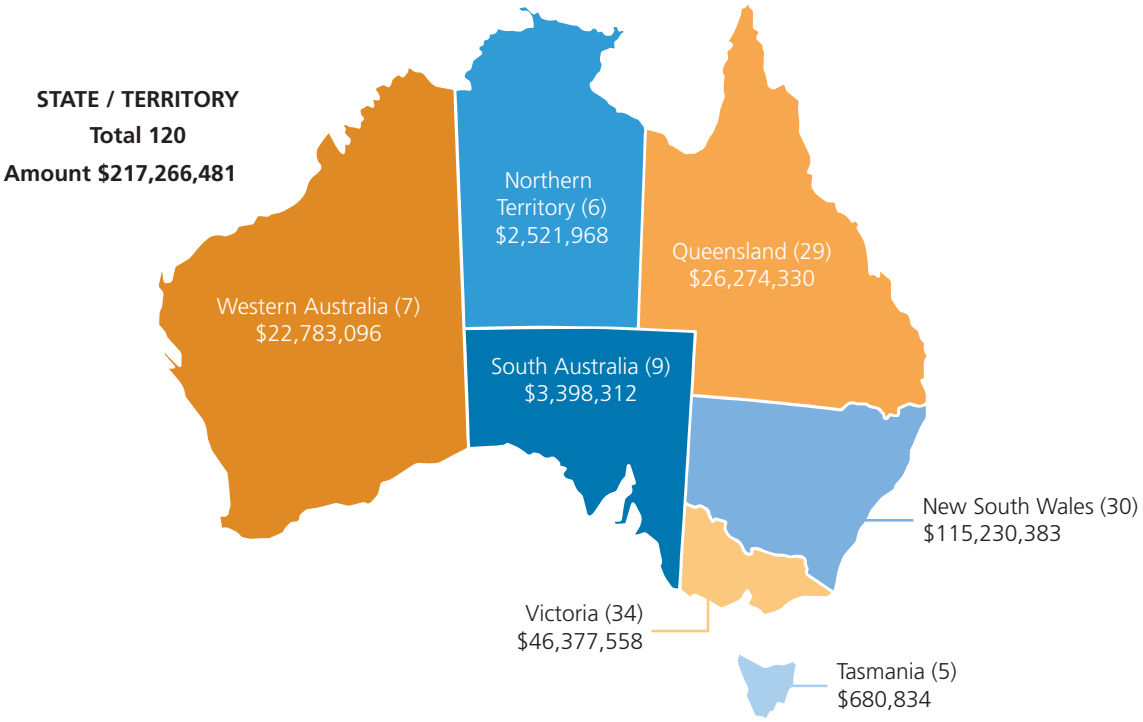

Figure 7 – Frauds by State and Territory

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 ten years, eight years three months, eight years and eight years.

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?'.

DURATION OF FRAUDS	NUMBER	AMOUNT	AVERAGE
Over 10 years	2	$5,354,548	$2,677,274
5 years up to less than 10 years	18	$100,278,751	$5,571,042
3 years up to less than 5 years	14	$26,300,981	$1,878,642
2 years up to less than 3 years	22	$26,398,186	$1,199,918
12 months up to less than 2 years	25	$41,212,941	$1,648,518
6 months up to less than 12 months	15	$12,562,316	$837,488
1 month up to less than 6 months	12	$1,991,838	$165,987
Less than 1 month	12	$3,166,920	$263,910
	120	**$217,266,481**	

Figure 8 – Time taken for fraud to be discovered

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 71 cases where evidence of how the frauds were discovered was available. Not all were specific. 24 referred only to an internal discovery.

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 eight specific references to the frauds being discovered whilst the perpetrator was on leave or after they had left the organisation. This figure could be underestimated due to the lack of further detail regarding the 24 internal discoveries. It is likely that some of these were also as a result of the staff member being away from their job for some reason.

One of the most concerning statistics is that 20 of the frauds were discovered by customers, who in turn notified the financial institutions.

Interestingly, nine perpetrators confessed. No doubt the deeds of some weigh heavily on their mind. Often perpetrators are relieved when they are finally caught as they are continually covering up their past and hoping that no-one finds out about it. This must be physically and emotionally draining.

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 where staff found the fraud by various means.

HOW DISCOVERED	INSTANCES
Internal discovery by staff *	24
Customer / Client notified organisation	20
Confessed	9
After they left the job / On leave	8
External audit	2
Internal audit	2
Other external party	2
Anonymous report	1
Report to Austrac	1
Partner of perpetrator informed	1
Police notified	1
Total	**71**

Figure 9 – How frauds were discovered

* Note that some of these internal discoveries may have been as a result of the staff member being away from their job. The information obtained could not conclusively identify the source of the internal discovery.

Specific examples of the ways the frauds were discovered included:

- 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
- Found while she was on maternity leave
- Referral from Star City to AUSTRAC concerning bets made by a gambler
- Turned herself in after her son questioned her about an unusual bank account
- Bank notified company of its concerns regarding suspect transactions

Warning signs that were ignored

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

- Gambling addictions
- Ignored company policy of staff not being allowed to arrange/approve loans to themselves and families or order loans in excess of $250,000
- Ignored policy of giving loans to themselves and families
- Lack of supervision and also needed no countersigning authorisation when ordering cash
- Reactivated the accounts of a number of former employees no longer with the company and altered their bank details
- The employee had unsupervised task of balancing and refilling the ATM in a large Melbourne city branch
- The employee is said to have accessed the banking computer system when her colleagues were logged on in their names
- Staff members altering customer addresses so the account statements went to their designated address
- Use of other staff members' passwords
- When customers queried the shortfalls he told them a mistake had been made and the money transferred back to their accounts
- She increased the value of her own land as security by 720%

What was the motivation?

Sometimes there is clear evidence of asset accumulation, lifestyle choices, financial pressures or a gambling addiction that can assist with determining the motive for a fraud.

Lifestyle improvement and gambling were by far the most prevalent reasons 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 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.

MOTIVATING FACTORS	NUMBER	AMOUNT	AVERAGE
Gambling	62	$90,860,355	$1,465,490
Improve lifestyle *	35	$107,124,344	$3,060,696
Financial pressures	12	$2,979,995	$248,333
Prop up failing businesses	3	$3,380,966	$1,126,989
Drugs	3	$2,504,000	$834,667
Other	5	$10,416,821	$2,083,364
	120	**$217,266,481**	

Figure 10 – Motivating factors

* 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.

Gambling as a motivator

More than half of the frauds in this research were motivated by a gambling addiction. Previous research studies have highlighted gambling addiction as a significant motivator in employee fraud.

In order to understand what forms of gambling were most attractive to the perpetrators, an analysis was undertaken of the modes of gambling. In 44 cases out of 62, the modes of gambling were identified.

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.

MODE OF GAMBLING	NUMBER	AMOUNT	AVERAGE
Poker machines	25	$26,780,833	$1,071,233
Casinos *	6	$14,435,583	$2,405,931
Horseracing	5	$33,530,424	$6,706,085
TAB	5	$5,456,826	$1,091,365
Multiple modes	3	$1,738,156	$579,385
Unknown	18	$8,918,533	$495,474
Total	**62**	**$90,860,355**	

Figure 11 – Main type of gambling that the proceeds of fraud were used for

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

Examples of the frequency of gambling or the amounts of money being gambled were highlighted during the court cases. These include:

- $160,000 on pokies
- Bookmakers flew him to Melbourne business class and was introduced to TV personalities and trainers
- Called telephone betting lines 59,000 times in four years
- Gambled $8.5 million at Star City. Was on Star City's top 100 turnover list and number three on list of top losers
- Had gambling debts of more than $100,000
- Had lost about $800,000 at Melbourne's Crown Casino and more than $200,000 on horse racing and internet gambling
- Hard working mother with pathological addiction to pokies
- He was in contact with many other gamblers, including Asian students and loans sharks at the Casino
- In the evening she would spend between $5,000 and $10,000 on the poker machines, playing two or three machines at a time
- Internet gambling debt of $17 million. He lost $11 million in 6 months alone and punted $48 million
- Lost $30,000 of own savings on pokies and tried to recoup losses
- Played the pokies five days per week
- Stole the money after she gambled her life savings on Pokies and Tattslotto and could not pay for a relative's kidney transplant
- 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

Lifestyle as a motivator

Lifestyle was the second biggest motivator for fraud.

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

- 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
- Overseas holiday, bought a house and two BMW cars worth $140,000. Bought furnishings and helped her in-laws to get out of debt
- Expensive cars, luxury goods and holidays
- Estimated $142,000 was spent on overseas trips or domestic holidays for herself and her husband; about $70,000 was spent on home renovations, another $55,000 on homeware and furnishings. Spent about $27,000 to lease a BMW car for her husband, while another $9000 went towards a car loan for his sister. About $8000 was spent on sports equipment
- He regularly splashed out on business-class flights to Thailand, where he would visit high-priced prostitutes and stay in five-star hotel rooms
- $100,000 BMW, a $70,000 Mini Cooper, French champagne and $320,000 worth of jewellery
- Fish tanks, a motorcycle, a shed, a trailer and to pay for renovations on an investment property
- $92,000 worth of telephone calls to psychics
- Spent the funds on buying cars, jewellery, a wine collection and luxury travel
- Used bank's money to speculate on shares and real estate

Impact of the frauds on the employers

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

This has included negative publicity, diversion of management and staff time, engagement of expert forensic accountants, legal expenses for recovery and increase in insurance premiums.

The bigger the financial institution, the larger the fraud has to be to have a significant impact. Large financial institutions 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.

The impact on the fellow employees of the perpetrators should not be underestimated. It is hard to quantify the emotional toll on those who were either interviewed as part of the investigation, did not identify the frauds earlier or were duped by the perpetrators.

The following comments by Judges and Magistrates illustrate this point:

'You took advantage of the fact that you were trusted by your colleagues, who would sign the necessary documents on your say so.'

'She has betrayed the personal trust placed in her by the account holders, and she has betrayed the trust placed in her by the bank by virtue of her position as manager, with overseeing authority to do many things without supervision or question.'

'This type of offending has a significant impact on public confidence in the banking industry. It has the potential of eroding public confidence in the banking system and to that extent adversely affects the reputation and standing of other employees in the banking industry.'

'You had unwitting bank workers sign forms to allow the transfer of money.'

Impact of the frauds on the perpetrators

Sentences

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 for large frauds. However, not every single person included in this research was sentenced to a gaol term.

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, the non-parole period.

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

AMOUNT DEFRAUDED	AVERAGE LENGTH NON PAROLE PERIOD	NUMBER OF OFFENDERS	NUMBER OF NON CUSTODIAL SENTENCES
Over $10 million	4 years 3 months	5	0
$5 million to $9,999,999	4 years	7	0
$1 million to $4,999,999	2 years 10 months	23	0
$500,000 to $999,999	2 years 4 months	21	0
$100,000 to $499,999	1 year 2 months	38	7
$50,000 to $99,999	10 months	12	2
Up to $49,999	10 weeks	17	10
		123	**19**

Figure 12 – Sentences after taking into account mitigating circumstances by amount stolen

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 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 included:

- Forfeited his pay and superannuation entitlements and began repaying the bank after obtaining work as a taxi driver
- Bankrupt. Depression
- Sold his home to repay some money
- Unemployed, having lost his position at the bank. He continues to rely on, Centrelink benefits
- His life is in tatters as a direct result of the offending. His relationship has broken down and he will go to gaol a bankrupt
- Borrowed her aunt's life savings to try to cover up the fraud
- Wife divorced him
- Depression and post traumatic stress
- Declared bankrupt
- Broke and being pursued by the bank for the money she embezzled
- Bankrupt and on anti-depressant medication
- Bank had frozen all her assets, including her home in Redfern, her car and the assets of her parents and her son, including all their bank accounts

What is consistent among the information provided to the courts is that the perpetrators suffered depression. Whether this was evident before their frauds, or subsequently became apparent, is unclear.

Not all people with depression commit fraud against their employer, yet it is a recurring issue that would be worthy of further research in the future.

Contact us

WARFIELD & ASSOCIATES

Warfield & Associates specialises in governance and the prevention, detection and investigation of unethical behaviour, including fraud and corruption and how to mitigate the risk and protect their brand, reputation and bottom line.

We provide fraud awareness training, undertake fraud risk assessments and forensic reviews. We also investigate allegations of fraud, corruption, financial crimes and other unethical behaviour or misconduct.

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 9230 7088
E-mail: info@warfield.com.au
Website: www.warfield.com.au