



## Fraud Minimisation

### 1. Introduction

Today I am presenting a topic which is getting a lot of attention at present. We have called the session "Fraud Minimisation" and I think this accurately reflects that although the risk of fraud can be significantly reduced, prevention of fraud is unachievable. If someone wants to rip you off, they will find a way.

The aims of the session are therefore to

1. Explain some risks specific to Medical Practitioners and Business Owners;
2. Discuss some actual cases that were identified in a review Cutcher & Neale conducted on a medical practice;
3. Outline the nature of internal control and why a strong control environment is important;
4. And finally to leave you with 3 steps that you can follow to reduce the risk of a fraud in your practice.

### 2. What is Fraud?

I thought we should start off with some definitions.

Barron's .....

Auditing Standard ASA240 .....

What is interesting about these definitions is that neither refers to money.

Whilst theft of money is the general perception of a fraudulent act,

- the theft of goods such as medical supplies,
- the authorisation of overtime on a timesheet that was never worked
- or the use of business assets for personal use such as telephones phones, internet connections, or postage
- or in the bigger picture the intentional misstatement of financial information

are all equally fraudulent as taking money from the banking or the petty cash tin.

It is also interesting to note that the Accounting Profession is addressing the increasing awareness of fraud by updating professional standards. The latest amendments clearly identify the business owner or management as having ultimate responsibility for prevention of fraud.

### 3. Has Fraud Been Committed Against You?

What was clear from the study is that there was a significant percentage of respondents who had NOT specifically addressed the risk of fraud.

The study was reported by KPMG in surveys conducted every 2 years regarding to incidence of fraud in businesses.



The report for 2008 recently released found that 50% of respondents believed fraud was a big problem for business but only 17% believed it was a problem for THEIR business.

#### **4. Has Fraud Been Committed Against You?**

Different businesses and industries have their own risk profile for fraud. The study showed that the most common types of fraud would apply to medical practices being false invoicing and theft of cash and stock.

Once a fraud has been identified it is unlikely that the business will recover the funds with the study reporting that on average 12% of the proceeds from fraud were recovered.

The low recovery of funds is in part due to the length of time between the fraud being committed and its detection.

#### **5. The Typical Fraudster**

There has certainly been an increase in frauds reported in local papers in the last few months and given some of the statistics in the fraud study discussed earlier, we could assume that for every fraud reported there are likely 10 more.

This slide shows some of the character traits that are demonstrated by people caught out.

In some of the cases reported in the press and some that Cutcher & Neale are aware form our audit work and investigations, the profile fits in many cases.

From my experience we have investigated more frauds conducted by women than by men although the studies show otherwise.

A recent examples highlights the simple methods and lack of controls.

In one instance, and like many employers, a business also maintained a separate social club bank account for employee contributions towards the end of year Christmas party and the like.

The bank account was not part of the business however the payroll employee was also a cheque signatory on the account. This allowed the employee to make deposits into the account as well as withdrawals with no separate review by any other employees of the balances.

The employee withdrew money from the account without being detected and then arranged for the actual costs of the Xmas party to be paid by the business in full which covered up for the withdrawal of funds from the social Club account.

In this instance the method was simple, the employee was a known gambler and also not part of management which also fits the profile.

#### **6. Why are Medical Practitioners at Risk?**

Auditors talk about inherent risk, and this is the risk of something going wrong due to the nature of the business.



Although these are generalisations, I feel there would be a good chance that some of these factors apply to each of your practices.

(Run through the risks for Medicos on the slide)

After investigating a fraud, in most cases we can identify “red flags” that in hindsight should have raised the suspicions of others within the organisation.

Behaviour

In some cases it will be the behaviour of an employee that may raise suspicions:

- They may be reluctant to take holidays;
- They may work long hours after everyone else has gone home; and
- They never delegate or share their responsibilities with other staff

These “people issues” can be the first signs that identify a fraud.

One example of this from experience was where one of my Partner’s at Cutcher & Neale was visiting his GP who was also a client. The Doctor introduced him to the receptionist as being the Doctor’s accountant. The receptionist thinking that the accountant was there for business, appeared very nervous and embarrassed. This reaction raised suspicions and the employee was soon after found to have been stealing from the Doctor.

## 7. Red Flags

A more in depth case study will help explain some of the risks that are present in medical practices.

The following “red flags” were identified by a review Cutcher & Neale conducted of a medical practice. We were not looking for fraud in particular, rather we were looking for evidence to support whether a detailed investigation was required.

We used specialised audit software to interrogate 5 years worth of data from the Practice Management Software.

Some of the results were:

- Gaps – this could indicate deleted records (2,698 gaps in consultation sequence)
- Unusual maximum fees – variances appear unusual as we would expect fees to be comparable for a particular service (2,914 nil fees)
- Unusual billing items – possible dummy transactions or amendments (69 billing items billed once in 5 years)
- Fee Adjustments – the level of fee adjustments appeared excessive possible alteration of receipts to line up with reduced bankings (5,586 adjustments over 5 years = 25 per week – value was \$69,000+)
- No explanation for fee adjustments – poor documentation is potentially a strong indicator that the amendments have not been authorised



## 8. Indicators of Possible Fraud (2)

- Variances in min and max fees – appears unusual – possible amendment of charges (33 fee types out of 221 had maximum fees that were more than 3 times minimum fees charged)
- High Debtors – possible that monies are not being banked (4,832 outstanding patient accounts = \$143,000+ and \$55,000 were > 2 years old)
- Variances in reports – strong indication that bankings is incorrect

Investigation of these items may not uncover fraud, but certainly these types of issues warrant close investigation.

So what can be done to address these types of problems?

## 9. Internal Controls

Internal controls are processes and procedures that have been communicated within the organisation to reduce the risk of unauthorised transactions being processed.

These controls can be related to the weaknesses that were detected in the review that we have just touched on.

For example:

- Completeness

Sequence numbers on documents, filing systems to ensure documents are filed in numerical sequence and regularly reporting and review of listings of receipts and payments would provide assurance that transactions were not missing or being hidden.

- Authorisation

Controls to require staff to sign reports evidencing their review, such as a payroll report being signed by the Practice Manager, independent of the preparer of the payroll.

- Segregation

Is one of the most effective controls as it ensures that no person is responsible for all steps of a process.

As an example the person receipting the money from the patient should not also control and reconcile debtors, perform the banking or prepare the bank reconciliation.

- Audit Trails

An audit trail is a record of the events that have occurred in the system.

It is particularly important that a computer system can produce an audit trail and these reports can be very effective in identifying unusual transactions.



These could include fee adjustments, deletion of entries, overriding fee schedules or writing off older debtors balances. The audit trail should identify the ID of the user who has initiated the change and this is particularly important in a system where a number of staff have access to the system.

- Effectiveness and review

Where segregation cannot be implemented, due to a lack of available staff for instance, review becomes more important.

Periodic review of reports and reconciliations by someone independent of the work provides a strong deterrent for staff contemplating fraud.

With respect to effectiveness, if the controls are not evidenced, such as by having a reviewer sign the report, you as owners cannot be sure that the controls has operated.

## 10. Fraud Minimisation

So after identifying the reasons why your practice may be at risk and some examples of cases where suspicions should be raised, there are 3 things that you should consider for your practice:

- Awareness

In too many cases the business owners consider the possibility of fraud to be low, it won't happen to them.

Our Firm has investigated more frauds in the last 12 months than in the last 10 years that I have been with Cutcher & Neale.

Principals and Practice Managers need to be aware of:

- your finances; and
- your staff and their behaviour
- Implementation of Internal Controls

Therefore as business owners and Managers you need to be able to rely on your systems and processes rather than the individual staff member who is performing the task.

Review the types of transactions that are undertaken and consider whether there are enough checks and controls in place.

1. Where possible implement procedures that ensure no one person is responsible for all processes.

This is referred to as segregation of duties

An example would be invoicing patients, receipting payments, preparation of the bankings and preparing the bank a debtors reconciliations.

2. Implement policies for checking of reconciliations and reports by staff independent of the person preparing the work.



This would be an authorisation control and would be useful where effective segregation of duties cannot be achieved

As Managers you can play an important part of the control environment by implementing strong policies and procedures for routine processes and a review structure that demonstrates a professional culture.

- Reporting and Review

Once you know what to look for, regular reporting by your staff and review of these reports can provide a significant increase in the level of controls within your practice.

The types of exceptions that were discussed earlier should be reviewed regularly, as well as:

- Banking summaries;
- Bank reconciliations;
- Patient debtors listings;
- Payroll reports;
- Cheque payment reports; and
- Bank transfer and EFT reports

With respect to reporting and review as a Principal you can either do this yourself on an ad hoc basis.

Practice Managers routinely review key reports. The existence of tight end of day, week and month procedures is an effective deterrent to fraud and improves the likelihood of identifying suspicious transactions.

For small offices where segregation of duties and effective review controls are not practical, rotation of staff duties provides an element of review that provides some reduction to the risk of errors or fraud.

Larger practices may seek some independent assurance around their control environment and risk of fraud.

## **Conclusions**

So overall we believe you can reduce the risk of fraud within your organisation by

- ◆ Increasing your awareness and that of your staff to the possibility of fraud;
- ◆ Implementing internal controls relative to the size of your practice;
- ◆ Increasing your understanding of reports produced by your systems and reviewing these on a regular basis; and
- ◆ Developing a culture that recognises fraud is a risk and communicates clearly the consequences for non-compliance the businesses approved policies and procedures

We have some time available to answer some questions.