A Review of Actual Fraud Cases in 2017

FRAUD REVIEW

mgi

AUDIT & ASSURANCE

Contents

Introduction

Fraud costs Australian businesses hundreds of thousands of dollars every year, and these are just the instances that have been detected.

Fraud can occur in any organisation, no matter what size, industry or sector. Fraud has been uncovered in the public and private sectors, in for-profit and not-for-profit entities, and in small, medium and large enterprises.

MGI's audit division helps its clients deter and detect fraud by staying abreast of current fraud cases in Australia. MGI works with clients to implement controls and safeguards to reduce the risk of fraud.

This fraud update is a summary of fraud cases uncovered by MGI Audit & Assurance and other exposed fraud cases in Australia during 2017. This update identifies the key factors that permitted the fraud to occur and provides recommendations to reduce the risks of these types of fraud in your business.

Stephen Greene
Director – Audit & Assurance

Fraud Snapshot

90%

Australian businesses targeted by email fraud in 2017, with 54% using ‘spoof’ email domain names.

72%

Small and medium sized business that do not believe that cyber fraud is a considerable risk to their business.

36%

Frauds in Australia carried out by an organisation’s own management.

30%

The increase in cyber crime and online scamming in 2017 versus 2016.

27%

The proportion of Australians that have been a victim of identity theft in 2017.

40%

Fraud in Australia takes place over a five-year period – detection is taking too long.

Case Studies | Credit Card Fraud

Background

- Involved the President of a large community-based organisation.
- The president made multiple personal purchases on his corporate credit card, including holidays, payment of his personal mortgage and payment of family members' monthly phone bills.
- The total cost of personal expenditure on the corporate credit card was in excess of $475,000 over six years.
- It is reported that the President's credit card statement was only queried once in an 11-year tenure.
- The internal accountant was in charge of reviewing the President's credit card transactions, but was unlikely to question transactions given the power held.

How did this fraud occur?

- No internal controls implemented within a high fraud risk area.
- The second reviewer of the President's corporate card was in a management position rather than another Board position (e.g. the Treasurer, member of the Finance Sub-Committee, etc.)
- Limited review of the profit or loss statement expense codes against budget, given that these expenses would have been recognised in one or more expense codes each year.

Frequency of the fraud risk

- The fraud occurred continuously across a six-year period.

How did this fraud get detected?

- A change in the CEO prompted a forensic audit into the expenditure of the organisation. Whilst the CEO was sacked by the Board, the investigation uncovered sufficient evidence for an independent review to be conducted.

How to reduce this fraud risk?

- Document and implement a credit card policy, clearly stating out the permitted uses and limits of each credit card holder.
- Ensure a detailed review of all credit card expenses is performed by an appropriate member of staff. For senior management credit cards, it is essential that the reviewer is of a sufficient seniority to be in a position to question any anomalies.
- Ensure all expenses are scrutinised against budget, and any variances are investigated.

Case Studies | Business Email Compromise Fraud

Background

- Business Email Compromise (BEC) fraud is one of today's greatest cyber threats.
- Involved a large private company CFO.
- Fraudsters took on the role of the CEO by hacking the company's email account and reviewing typical requests for payment made by the CEO to the CFO.
- Fraudsters created a fake chain of emails between the CEO and the Board, appearing to approve the transfer of funds to a nominated bank account for a deposit on new machinery.
- The CFO made the transfer as the email requested to the fraudulent bank account.
- While a control had been implemented for the CFO to require a second authoriser in bank transfers, the finance manager was on leave and left their online bank details and passwords with the CFO (their immediate line manager).
- This was not covered by the company's insurance, and the amount paid was lost by the Company.

How did this fraud occur?

- Email requests accepted at face value.
- No secondary communication set up confirming bank transfer requests.
- Dual authorisation control of bank payments/ transfers was not followed.

Frequency of the fraud risk

- According to the latest statistics on BEC fraud, 90% of all Australian businesses have experienced BEC attempts in 2017.

How did this fraud get detected?

- The payment of the deposit was highlighted in the monthly finance meeting with the Finance Sub-Committee and noted that it was bogus.
- The fraud was therefore only detected after the event occurred, without the chance of the company recovering the amount paid.

How to reduce this fraud risk?

- All bank payments and transfers should pass through the standard accounts payable procedures, ensuring documentation is available to support all bank transactions.
- In the event that miscellaneous bank transfers are permitted (by senior management or an owner), a secondary communication check should be provided prior to approval, e.g. an email request should be followed-up by a telephone call.
- Dual signatory control on all bank payments should be followed at all times, with pre-approved limits for each level of authority approved by the Board.
- IT controls are implemented, such as Domain-based Message Authentication, Reporting and Conformance (DMARC) software, highlighting potential fraudulent attempts of your email systems.

Case Studies | Payroll Fraud

Background

- Involved the payroll clerk of a large private business.The payroll clerk had been with the organisation for more than fifteen years.
- The payroll clerk had full autonomy to run payroll transactions, change pay rates, add new employees and transact leave entitlements.
- The clerk set up duplicate employees in the payroll system with the exact names of current employees at the time (e.g. two John Smiths).
- The bank account details of one of the names were legitimate. However, the second duplicate employee's salary would be paid into the payroll clerk's personal bank account.
- While final pay-run checks were performed by senior management, this was an overall reasonableness review and not line-by-line, as the business had over 80 employees.

How did this fraud occur?

- Over-reliance of trust placed on one payroll clerk to perform all payroll transactions.
- Payroll clerk continued to perform payroll duties remotely, even when on annual leave (at the clerk's request).

Frequency of the fraud risk

- This fraud occurred on multiple pay-runs over multiple years until detected.
- While this fraud is internal, it is likely that this fraud would continue to occur until detected, or until the employee left the organisation.

How did this fraud get detected?

- Computer Assisted Audit Techniques (CAATS) recognised duplicate payroll names in the payroll audit trail.

How to reduce this fraud risk?

- Ensure segregation of duties within payroll processes.
- Implement spot-checks of individual pay-runs, ensuring a sample of employee details are vouched back to their employee file (including pay rates, bank account details, etc.).
- Request that final pay-run reports to be reviewed by management are printed in alphabetical order to highlight duplicate employees more easily.

Related fraud cases

- In addition to duplicate employees, fictitious employees being set up in the system is also a risk (particularly for businesses with a large number of employees). Spot-checks by a secondary reviewer back to employee files will reduce this risk.

Case Studies | Supplier Fraud

Background

- Involved a small-to-medium enterprise (SME).
- A request was received via email posing as one of the business' suppliers notifying them that they had changed bank account details.
- The bogus email received from the supplier matched the exact email logos, footers, disclaimers etc. of the supplier's actual email tag (that the accounts clerk was familiar with).
- The accounts clerk changed the supplier's bank details in their system without any additional checks or processes, and the company made a number of payments to the fraudulent bank account.

Frequency of the Fraud Risk

- This fraud instance resulted in four payments made to a fraudulent bank account over the space of two weeks.
- This external fraud risk is likely to continue to occur until detected.

How did this fraud occur?

- No secondary controls were implemented for supplier bank account amendments.
- Email requests from associates were accepted on face value.

How did this fraud get detected?

- The company's bank notified them that the new bank account of the supplier was high risk and to confirm the transaction with the supplier.
- Upon a secondary check was performed with the supplier, it was found that the bank account request was fake.

How to reduce this fraud risk?

- Ensure controls are implemented within the accounts payable process for changes to supplier details, especially bank account amendments.
- If requests are received via email (no matter how legitimate the may appear), confirm the request with a telephone call to the supplier contact.
- If requests are received via telephone, request that an email/letter is sent to confirm authenticity.
- Regularly reconcile accounts payable ledgers with supplier statements to investigate any discrepancies.

Outlook for 2018 | Cyber Fraud on the Rise

While the rates of cyber fraud are already alarmingly high, the Australian Government estimates that all types of cyber fraud will continue to rise, and become the "new norm".

Especially at risk are small and medium-sized business according to the Reserve Bank's Cyber Security Chief, who believes fraudsters are turning their attention to "easier prey" at the smaller end of town.

Smaller businesses are less likely to take cyber fraud risks as seriously as larger listed organisations, and therefore likely to have weaker preventative controls against common cyber fraud techniques such as email phishing, ransomware and identity theft to name but a few.

While cyber fraud attempts are now unfortunately inevitable for most Australian businesses as we move into 2018, it is essential that all organisations understand the risks of cyber fraud and plan accordingly.

The key areas we advise our clients to consider with regards to cyber fraud are as follows:

Education and Training

Most employees of small and medium-sized business are acutely unaware of the risks that may unfold if they open a fake speeding ticket invoice attachment from the Australian Police or fake energy bill from Origin. Providing basic training to your staff on the types of common cyber fraud out there will be money well spent in protecting your business from this ever-increasing risk.

Detection and Prevention

Detecting cyber fraud and implementing controls to prevent future attacks is essential in the war against cyber fraudsters.

Detecting cyber fraud starts with implementing and documenting detailed internal financial and accounting controls. Remaining vigilant and questioning all variations to your internal policies will highlight that bogus request from a supplier to change bank details, or the email request to transfer money to a designated account.

In addition, your IT policies and procedures must have standard controls such as regular penetration tests, sophisticated user passwords and phishing detection software to detect any cyber breaches.

IT controls should also cover preventative measures, such as sufficient and up to date virus and firewall software.

Outlook for 2018 | Cyber Fraud on the Rise

Disaster Recovery

If the first two areas fail, then having sufficient disaster recovery systems is essential to reduce business disruption and loss of data.

For example, if back ups are being taken to a cloud server every 15 minutes and an employee accidentally opens a phishing email with a ransomware attachment, the business can be up and running on the back up version within the hour with only minimal loss of data.

Disaster recovery is, therefore, the final line of defence in an ever-increasing cyber fraud environment.

Key tips when reviewing your disaster recovery systems:

Ensure your disaster recovery system is documented in a jargon-free policy that all the Principles of the business can understand and follow. If your IT Manager is on a beach in Florida when a cyber fraud event occurs, there needs to be a second option.

Ensure your data back ups occur regularly. Having backs ups only occurring once a day still leaves your business open to business disruption in the event of an attack. We recommend back ups should be taken as regular as possible to reduce this risk.

Test your disaster recovery process! We recommend testing a full system recovery at least annually. If you have external IT providers, ensure they are testing this and providing confirmation reports on the success of the restoration regularly.

Summary

The level of sophistication of current day fraud requires boards and management to improve their internal controls and ensure their organisations are well placed to deter and detect fraud.

Fraud can occur in any organisation, no matter what size, industry or sector. Fraud has been uncovered in the public and private sectors, in for-profit and not-for-profit entities, and in small, medium and large enterprises.

Our recent experiences with fraud has highlighted IT risk as the fastest growing fraud risk for organisations, due to the increasing reliance on information technology, paperless financial systems and cloud-based software. This increasing reliance has also increased the fraud opportunities to target businesses whose IT controls have not been upgraded to match their usage.

It is essential that your organisation implements and documents sufficient internal controls to prevent and detect all potential types of fraud that may impact your business. This starts by having experienced auditors assisting your organisation to highlight all potential fraud risks.

Speak to one of our team today about our free IT Cyber Fraud Healthcheck, which will uncover any potential weaknesses to your current cyber fraud controls and recommendations for improvement.

Get in touch

Stephen Greene
Director – Audit and Assurance

Mobile	0426 510 812
Email	sgreene@mgisq.com.au

Graeme Kent
Director – Audit and Assurance

Mobile	0414 828 812
Email	gkent@mgisq.com.au

mgi
AUDIT & ASSURANCE

This publication contains general information only and MGI Audit and Assurance is not, by means of this publication, rendering accounting, business, financial, investment, legal, tax, or other professional advice or services. This publication is not a substitute for such professional advice or services, nor should it be used as a basis for any decision or action that may affect your organisation. Before making any decision or taking any action that may affect your business, you should consult a qualified professional advisor. MGI Audit and Assurance shall not be responsible for any loss sustained by any person who relies on this publication.