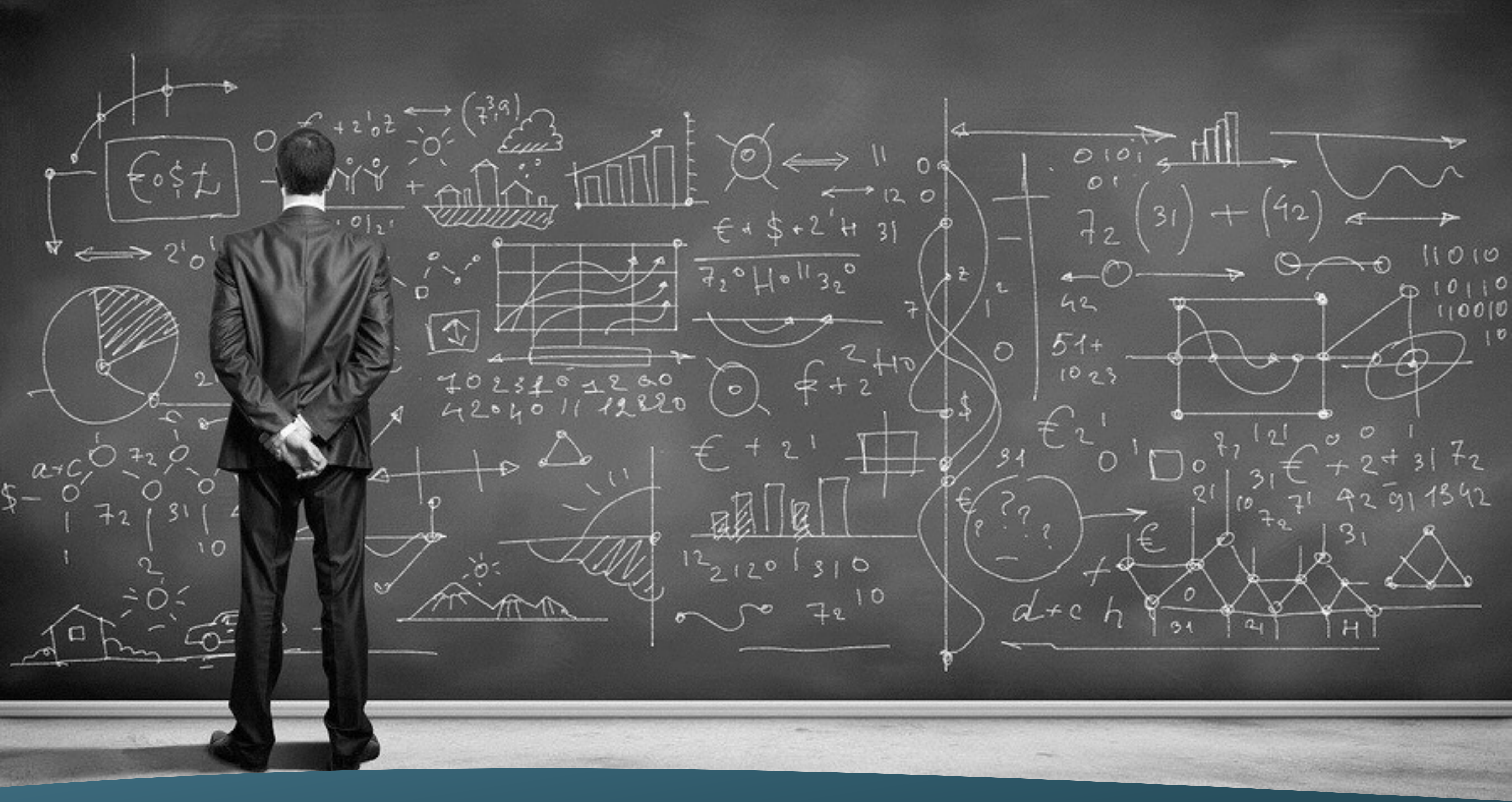


Fraud Review 2015

A Review of Actual Fraud Cases in 2015

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.

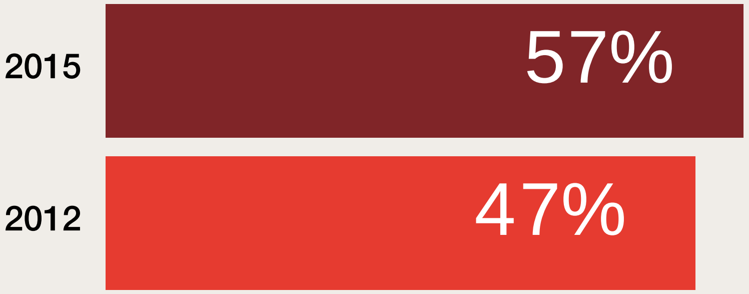
MGI's audit division helps its clients deter and detect fraud by staying abreast of current fraud cases in Australia. MGI works with clients to implement controls and safeguards to reduce the risk of fraud.

This fraud update is a summary of fraud cases uncovered by MGI Audit & Assurance and other exposed fraud cases in Australia during 2015. 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.

Fraud Snapshot

of Australian Organisations experienced in excess of 10 fraud incidents in the past 24 months.

Percentage of Australian organisations that have experienced crime.

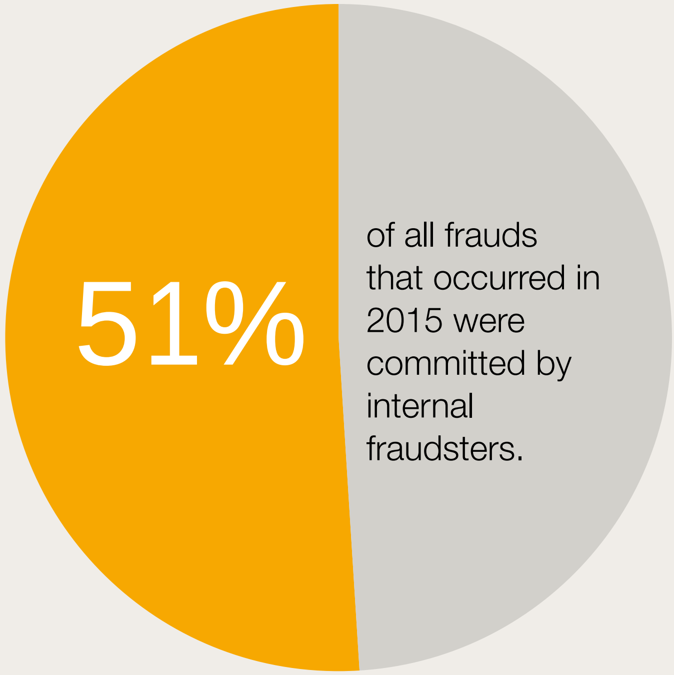


Top 5

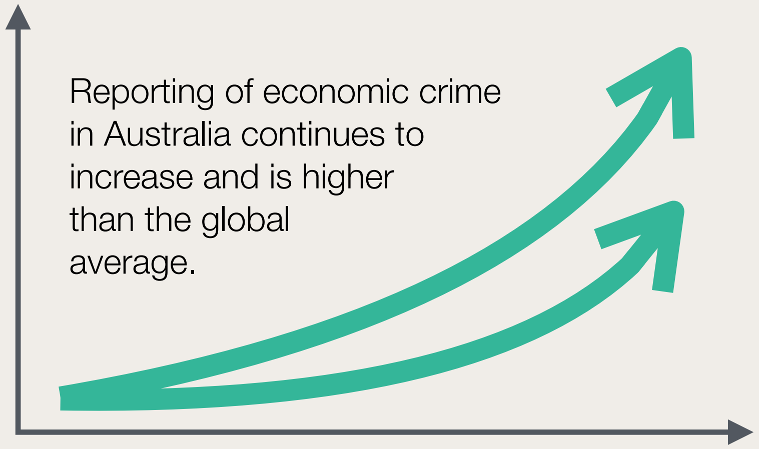
The big 5 fraud types (in order) are:

1. Asset Misappropriation
2. Cybercrime
3. Procurement Fraud
4. Accounting Fraud
5. Bribery

Tip offs are still the best detection of fraud, followed by fraud risk management and detection from the auditor.



of all frauds that occurred in 2015 were committed by internal fraudsters.



Reporting of economic crime in Australia continues to increase and is higher than the global average.

Source: Association of Fraud Examiners, PWC and KPMG.

Case Studies : Overpayment Fraud

Background

- Involved the Finance Manager of a major regional council in Queensland.
- The Finance Manager was close to retirement and had been in the position for more than 10 years.
- Late one evening, the Finance Manager deliberately overpaid a creditor invoice.
- The Finance Manager contacted the supplier the following morning and apologised for the over-payment. The Finance Manager requested for the over-payment to be refunded into a separate bank account (the Finance Manager's personal bank account). Due to their long-standing relationship, the supplier did not question this with the Finance Manager.
- The Finance Manager repeated this fraud with two additional suppliers during the same financial year. The total fraud was estimated to be in excess of $1 million.
- The council had a second signatory control on bank payments, however the review was not performed with sufficient detail.

How Did This Fraud Occur?

- Over-reliance on key positions within the finance team.
- Lack of segregation of duties within payment processing.
- No reconciliations performed of supplier statements back to the general ledger.
- Second person reviews of bank payments not performed with any detail (eg: line-by-line back to supplier invoice).

Frequency of the Fraud Risk

- In this instance, the fraud occurred three times.
- Frauds of this type are more easily detected and are likely to be one-offs (unless fake purchase invoices are raised to offset the over-payments in the system, or the overpayment is 'general journalled' to a profit and loss account).

How Did This Fraud Get Detected?

- The external auditors performed sample checks between the supplier statements and the balances per the accounts payable ledger and noticed large negative balances.
- These were investigated and traced back to over-payments from the company bank account.
- Upon questioning, the Finance Manager confessed to all cases.

How to Reduce this Fraud Risk?

- Ensure all of your organisation's bank payments require at least two separate senior members to release funds.
- Ensure each bank authorisers are instructed to review transactions line-by-line back to supporting documentation. Question any variances!
- Ensure accounts payable clerks reconcile supplier statements back to your trade payables ledger and review all variances.

Case Studies : IT Fraud

Background

- Involved a small-to-medium enterprise (SME).
- The Managing Director would regularly email the Financial Controller to transfer money from the business account.
- A replica email was fraudulently sent to the Financial Controller, purportedly from the Managing Director, requesting a transfer of funds.
- The replica email had one domain name character different to the actual domain name, but crucially the contact name (eg: the name that appears in the inbox if the email address is in your address book) was exactly the same as the Managing Director's name.
- The Financial Controller sent the funds to the requested fraudulent bank account without any secondary controls or checks.

How Did This Fraud Occur?

- Email requests accepted on face value.
- No secondary communication set up confirming bank transfer requests.

Frequency of the Fraud Risk

- This fraud instance was a one-off as it was detected. However as this fraud is external, it would likely occur until it was detected.

How Did This Fraud Get Detected?

- The organisation's bank contacted the Financial Controller confirming the transfer, notifying them that the account that the funds were being transferred to was deemed to be a high risk.
- A secondary check was performed with the Managing Director who confirmed the request was bogus.

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, eg: an email request should be followed-up by a telephone call.

Case Studies : Payroll Fraud

Background

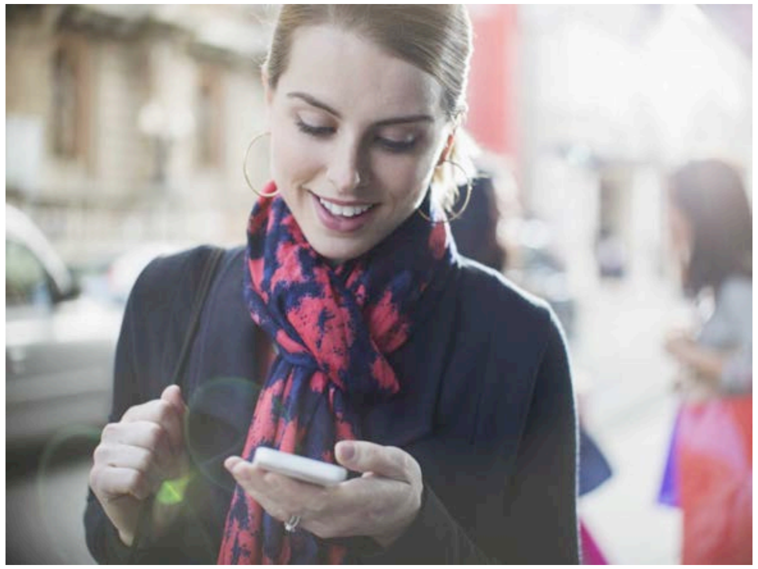
- Involved the payroll clerk of a large private business.
- The payroll clerk had been with the organisation for more than fifteen years.
- The payroll clerk had full autonomy to run payroll transactions, change pay rates, add new employees and transact leave entitlements.
- The clerk set up duplicate employees in the payroll system with the exact names of current employees at the time (eg: two John Smiths).
- The bank account details of one of the names was legitimate, however the second duplicate employee's salary would be paid into the payroll clerk's personal bank account.
- Whilst 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.
- Whilst 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).
- 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 2016 - Digital Banking

Banking fraud in Australia is on the rise. Fraud rates per $1,000 increased 26% from 2013 to 2014 and are forecast to increase again for 2015/16. One of the main factors in increased banking fraud is Australian's use of technology to make banking transactions.

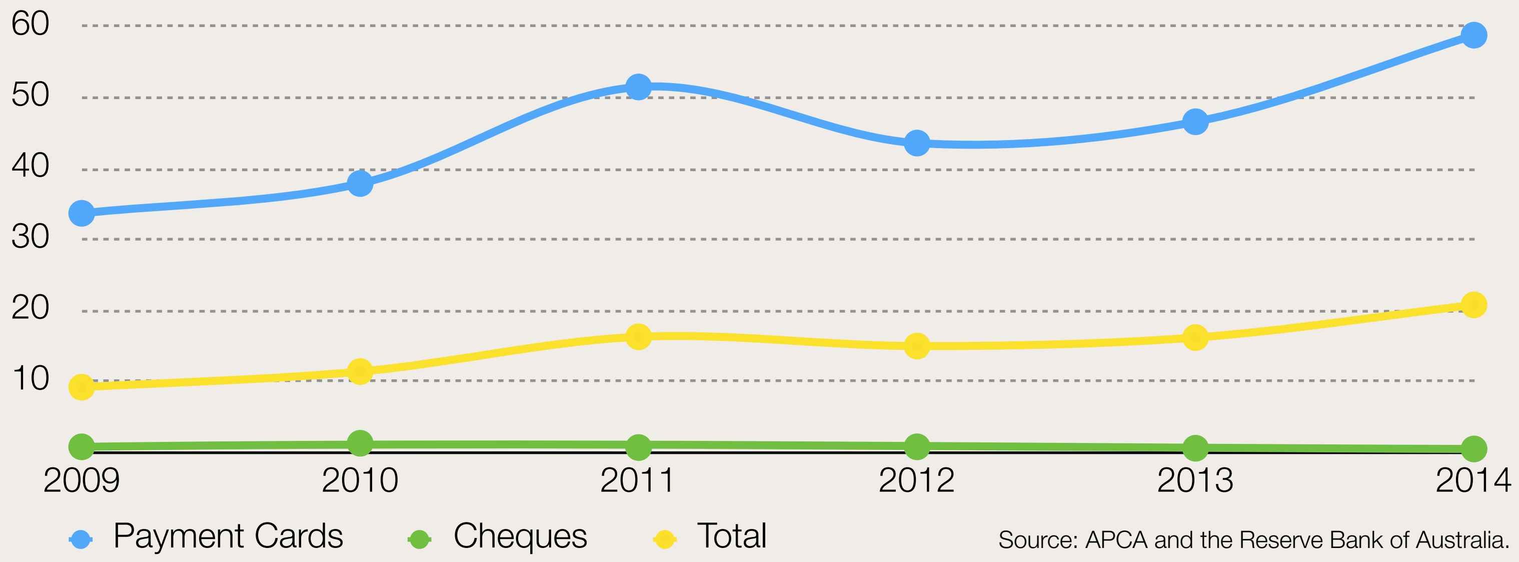
According to a global survey by Google, Australia has one of the highest smartphone penetrations in the world at 37 per cent – just behind Singapore – and we're also consuming more applications (apps) than the US or Britain.

The research noted we're also leading the way in mobile banking, with Australians 65 per cent more likely than the British and 14 per cent more likely than Americans to conduct banking on our phones. And by 2016, mobile payments are expected to reach $US617 billion worldwide – that's nearly a sixfold increase from 2011 at $US105 billion.

Whilst banks have implemented strong security measures to protect your business accounts, fraudsters see opportunities whenever money is handled. So how will fraudsters target you in the ever evolving digital age?

- Malware – You may inadvertently download software that can monitor and record your keystrokes, including confidential internet banking passwords and logons.
- Social Media – Popular social media are places where fraudsters can harvest information about potential targets. Social media default privacy settings are typically insufficient to provide sufficient privacy safety, and you may be at risk at criminals obtaining personal information such as addresses, phone numbers and your date of birth.
- Phone Porting – By harvesting personal information, fraudsters can request smartphone providers to switch or 'port' a victim's phone number to a new device. The fraudster may then send messages to the victim (posing as the victims smartphone provider) advising them of technical difficulties, which buys them more time to extract sensitive data from your phone.

Australian Cards and Cheques - Fraud Rates (cents per $1,000)



Source: APCA and the Reserve Bank of Australia.

Outlook for 2016 - Digital Banking

Security Tips

- Use only official apps – make sure to only use apps supplied by your financial institution and only download them from official app stores.
- Protect your tablet and smartphone – install and keep up-to-date anti-virus and firewall software purchased from trusted suppliers. It is important to update the software because new viruses emerge for which software providers create new barriers to deal with the new threats.
- Protect your passwords – ensure you keep confidential your PIN and Internet banking logons and passwords. Avoid using the same login passwords for multiple websites, especially when it enables access to websites that include sensitive personal information. Set a pass code for your device and a PIN for your SIM. If your banking app allows login with a PIN, make sure it is different to the one used to unlock your mobile device. Make sure your password or code is something that's hard for others to guess but easy for you to remember.
- Read privacy policies – before you provide personal information to any website, understand how your information will be used and how long it will be retained.
- Be wary of free downloads, programs, software or screensavers – sometimes malware and spyware can be hidden in free offers of other files.
- Beware of hoax e-mails – be alert to offers that are "too good to be true" or are designed to elicit an emotional response and triggers the thought of sending money. Always question messages that come out of the blue and verify the authenticity through trusted channels. Do not respond using information or links provided in the original message. No bank will ever send customers an e-mail with a link to online banking or ask for confidential information, so treat with suspicion any unsolicited e-mail that appears to be from your bank.
- Always log out of Internet banking sessions once you've finished.
- Wi-Fi – don't conduct Internet banking using unsecured Wi-Fi networks.

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.

The average fraud incident costs SME business in excess of $15,000. For small to medium businesses this can have significant long-term repercussions. To identify any fraud risks currently at play in your business, take our fraud questionnaire from the following link: http://www.mgisq.com.au/surveys/fraud_questionnaire

Or speak to one of our team today.

Stephen Greene
Manager - Audit & Assurance

Phone	07 3002 4800
Mobile	0426 510 812
Email	sgreene@mgisq.com.au

Graeme Kent
Director - Audit & Assurance

Phone	07 3002 4800
Mobile	0414 828 812
Email	gkent@mgisq.com.au

Website	www.mgisq.com.au