Risk Consulting

IIA-AUSTRALIA TECHTALK LIVE WEBINAR: FRAUD RED FLAGS IN A DISRUPTED ENVIRONMENT

Monday 27 July 2020

By Roger Darvall-Stevens, Partner and National Head of Fraud & Forensic Services, RSM Australia

RSM

What we will cover

- Overview of the current fraud environment and why fraud activity may be increasing
- Understand the various types of red flags and how these indicators can help detect fraudulent behaviour
- Ensuring conformance / compliance with various local and global fraud standards and legislation
- Identifying current high-risk fraud areas
- Determining methods to strengthen your organisation's fraud control framework
- Procedure to undertake when fraud is uncovered

Who am I and who to contact?

Roger Darvall-Stevens

Partner, National Head of
Fraud & Forensic Services

RSM Australia

T 0421 056 683

roger.darvall-stevens@rsm.com.au

www.rsm.com.au

Milind Sheth

Senior Manager,
Fraud & Forensic Services

RSM Australia

T 0430 114 461

milind.sheth@rsm.com.au

www.rsm.com.au

Who am I and who to contact?

Roger Darvall-Stevens, Partner, RSM Australia

Roger is the National Head of Fraud & Forensic Services, Australia, at RSM Australia. He has over 30 years of experience in forensic accounting, forensic investigations of a range of matters (e.g. fraud, bribery, corruption, and workplace improper conduct such as bullying and harassment), fraud and corruption control (prevention including training, detection, response, and foreign bribery and corruption compliance advice), forensic technology (forensic IT and forensic data analytics), operation of whistleblower reporting avenues and management advice, and forensic due diligence.

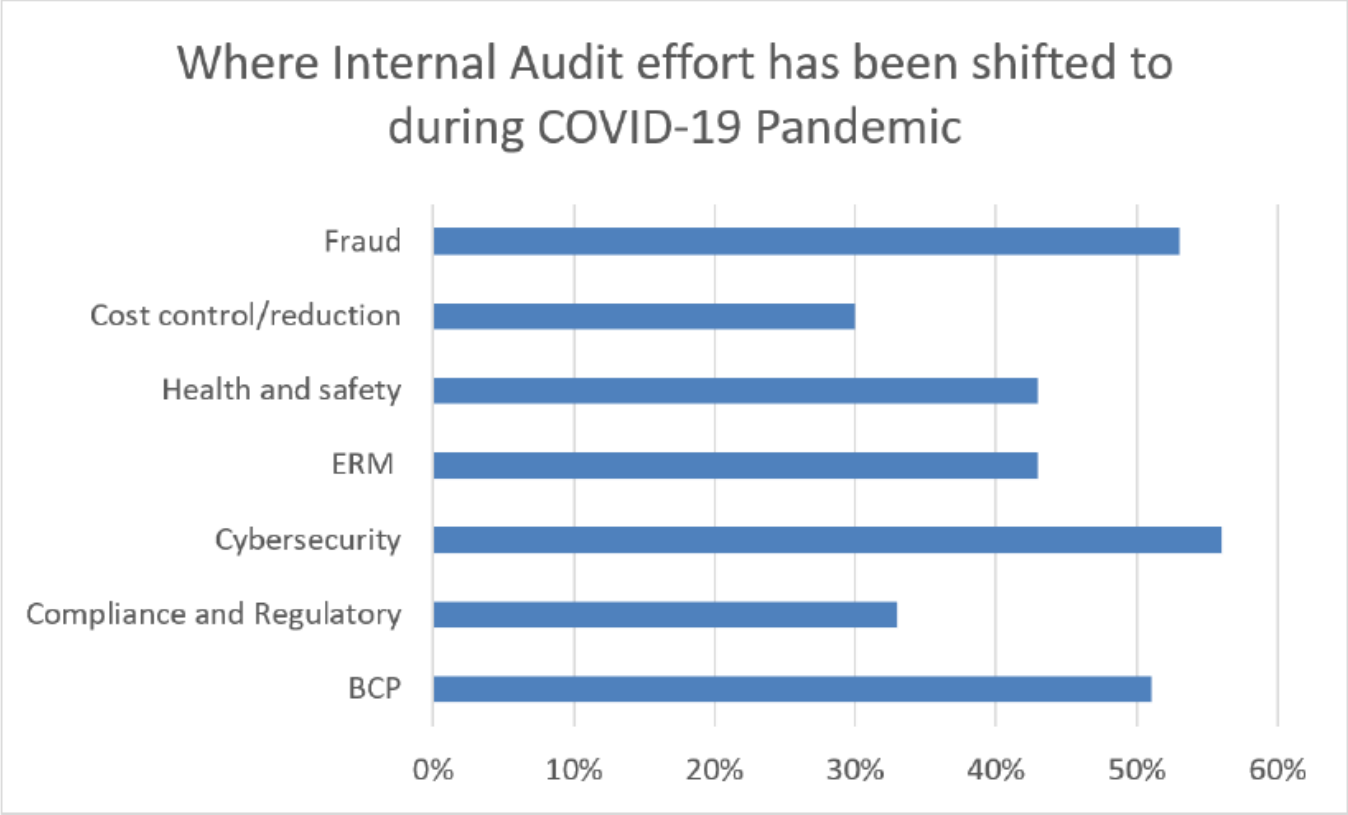
Roger is MBA and MA (Criminology) qualified, a licensed investigator in multiple locations across Australia and New Zealand, a former police detective (included fraud, and counter-terrorism), a CFE (Certified Fraud Examiner) and Regent Emeritus (Board member on the Association of Certified Fraud Examiners [ACFE] global Board 2012-2013), Authorised Trainer for the ACFE, and trained and practiced in advanced interview techniques. Prior to RSM, he was a Partner in forensics for a 'Big 4' firm (EY) where he was for 13 years, and also previously held similar roles in the private sector. Roger regularly presents at international and local conferences and seminars including previously at the RSM Asia Pacific Conferences, and has authored related articles and publications.

What we will cover

- Overview of the current fraud environment and why fraud activity may be increasing

IIA-Australia COVID-19 Survey, 9 July 2020

The graph shows where respondents have seen audit effort focussed during the pandemic.



What can businesses do including WFH risk mitigation

Access our RSM Australia article on ‘RSM’s Anti-Fraud and Corruption Toolkit for Business’ by emailing me / accessing our RSM website at:

https://www.rsm.global/australia/insights/technology-and-risks/covid-19-anti-fraud-and-corruption-toolkit-business

CORONAVIRUS (COVID-19) PANDEMIC

ANTI-FRAUD AND CORRUPTION TOOLKIT FOR BUSINESS

Amid widespread public concerns over the rapidly changing COVID-19 situation, fraud, corruption and workplace misconduct risk is heightened. There has been an escalation in fraud related to the COVID-19 pandemic, which puts businesses at risk of further loss and reputation issues. Now is not the time to ignore governance, risk and compliance measures designed to mitigate these risks but for management to be ever-vigilant and take action like conducting a RSM COVID-19 pandemic anti-fraud/corruption and workplace misconduct review. It was not until these crises are over (like the 2008 global GFC) when the fraud skeletons emerge. Be proactive!

Why be alert, not alarmed, to fraud, corruption and workplace misconduct during the Coronavirus pandemic?

The global and local Coronavirus (COVID-19) pandemic has created many changes to our workplaces and the way we do business. This also brings along new or heightened risks including the risk of fraud, corruption and workplace misconduct that will further impact a business's performance. This resulting potential financial and / or reputation loss will be felt by the business regardless if your business is global or local, or private sector / a company or a government organisation.

The following is what we know about the impacts from similar global events (such as the 2008 Global Financial Crisis or GFC, and natural disasters) of fraud, corruption and workplace misconduct about these times from similar events:

1. Fraudsters will prey on business and individuals in times of crisis, hoping the usual internal control defences and professional scepticism are down.

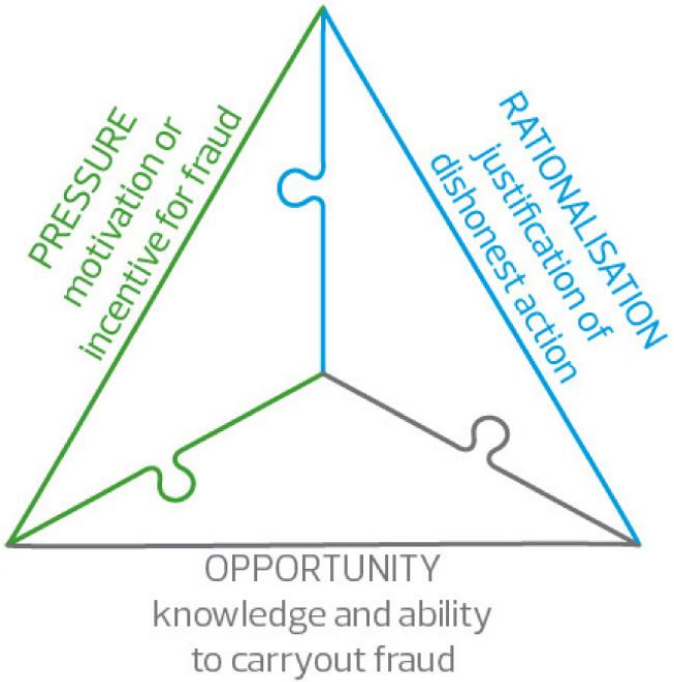
by criminologist Dr Donald R. Cressy in the 1950s but still as relevant today. In summary, for fraud, corruption or related workplace misconduct to occur are three elements present – motive, opportunity and rationalisation. In times of crisis, an employee(s) may exhibit financial stress or hardship as a result of job losses from household members during the current COVID-19 pandemic, or even from fear of their own job loss (even if only a perception or fear, and not a reality). These stresses may motivate fraudulent behaviour. An employee(s) may rationalise that they deserve extra money due to their hard work or length of services and may therefore justify stealing from the business, and the opportunity may exist if internal controls and management review is not vigilant and diligent.

Why be alert, not alarmed, for fraud, corruption and workplace misconduct

- What do we know from COVID-19 similar global crisis events (e.g. 2008 GFC, and natural disasters)?
  - Fraudster will prey on business and individuals in times of crisis, hoping that usual internal control defences are lax
  - Internal controls may be circumvented for expediency to keep business processes operating or govt. assistance to private sector
  - Management review may not be as vigilant due to distraction by COVID-19 and other management responsibilities
  - The fraud triangle is the best insight to the circumstances leading to fraud, corruption and workplace misconduct

Understanding why it occurs in these crisis times

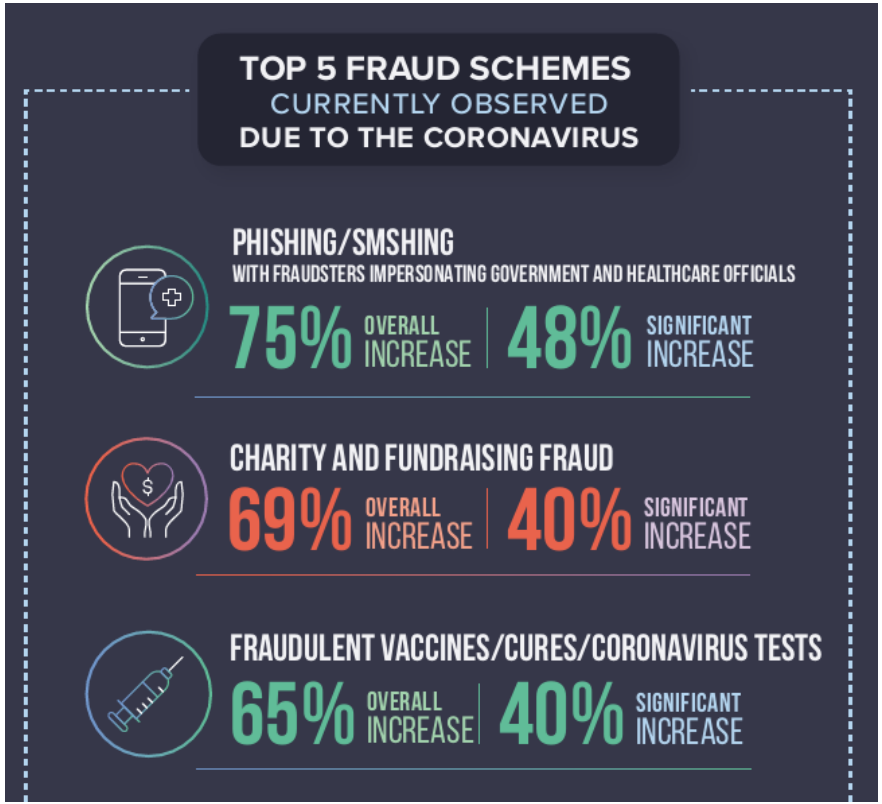
- First espoused by criminologist Dr Donald R. Cressey in the 1950s
- Still just as relevant today
- All 3 elements must be present for fraud, corruption or improper conduct to occur
- e.g. in crisis times:
  - **Motivation** through financial stress / hardship / job loss fear
  - **Rationalisation** that "I deserve it / extra money due to my hard work or loyalty"
  - **Opportunity** as internal controls or management review are not vigilant or diligent



Who has heard for the ACFE?

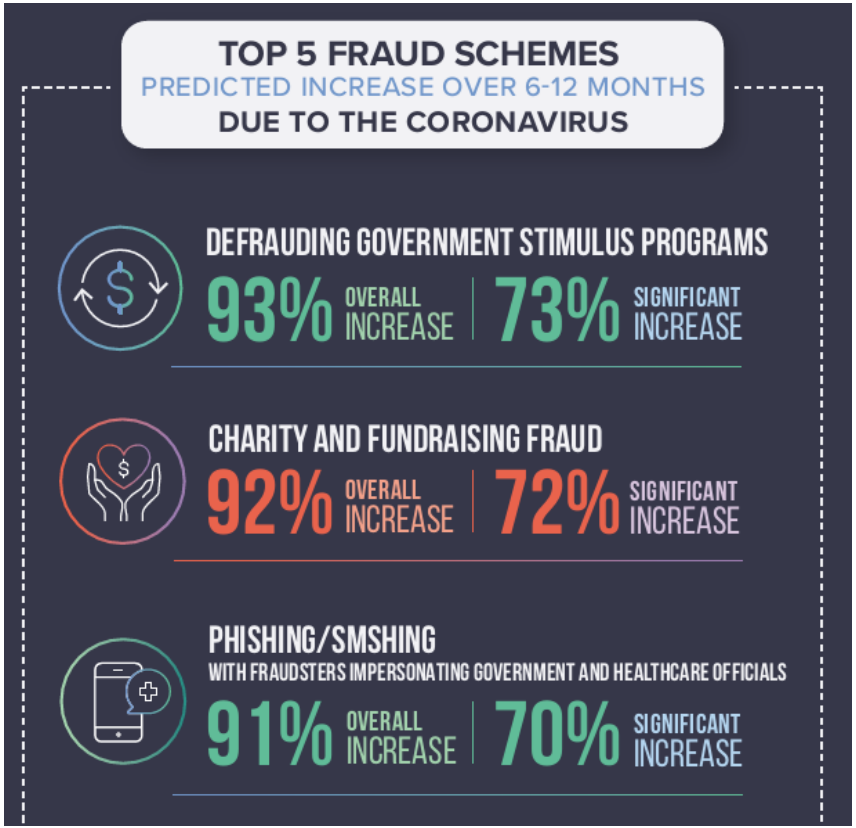
- The Association of Certified Fraud Examiners
- Pre-eminent global anti-fraud professional association
- 85,000 members in over 180 countries
- www.ACFE.com (free info. without being a member)
- CFE (Certified Fraud Examiner) global certification for anti-fraud professionals
- Produces two yearly Global Fraud Study

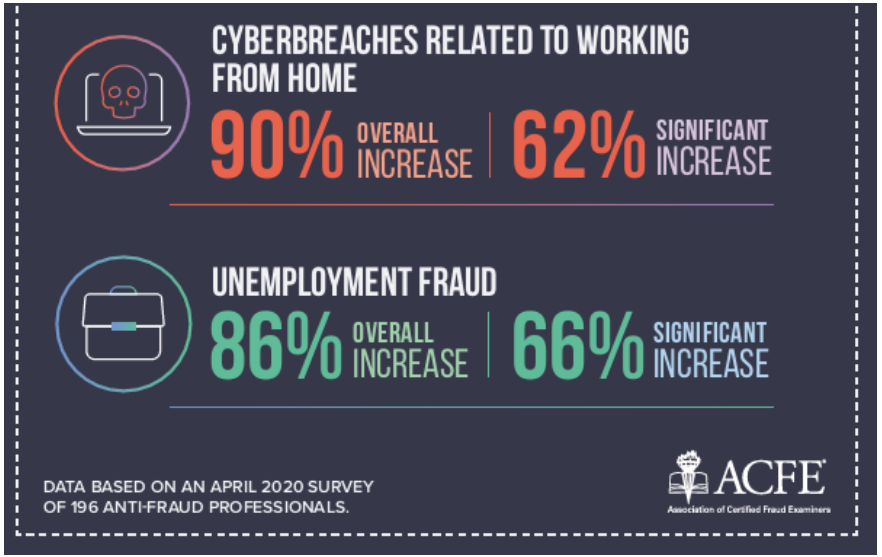
Current COVID-19 fraud schemes (Source: ACFE)



RSM

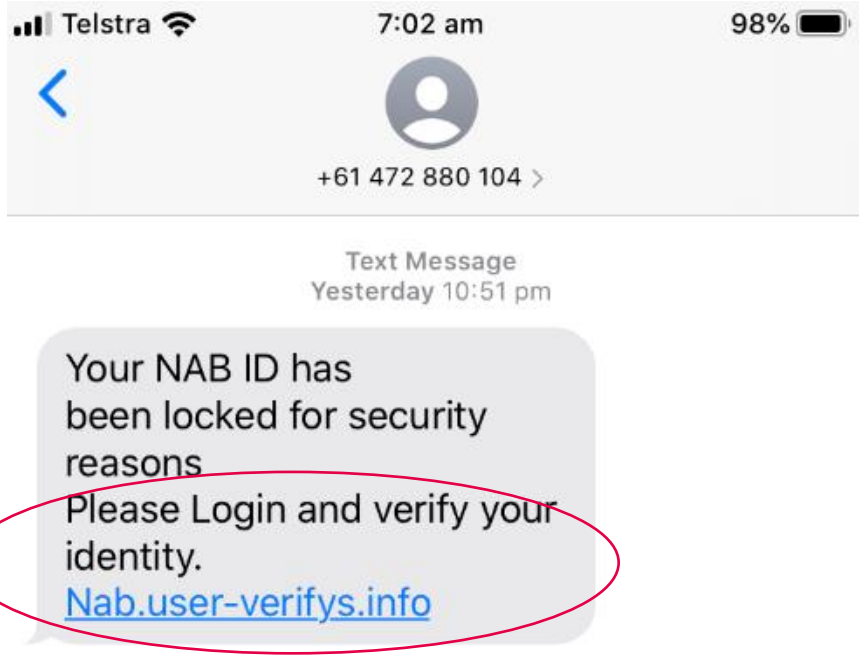
Predicted COVID-19 fraud schemes (Source: ACFE)



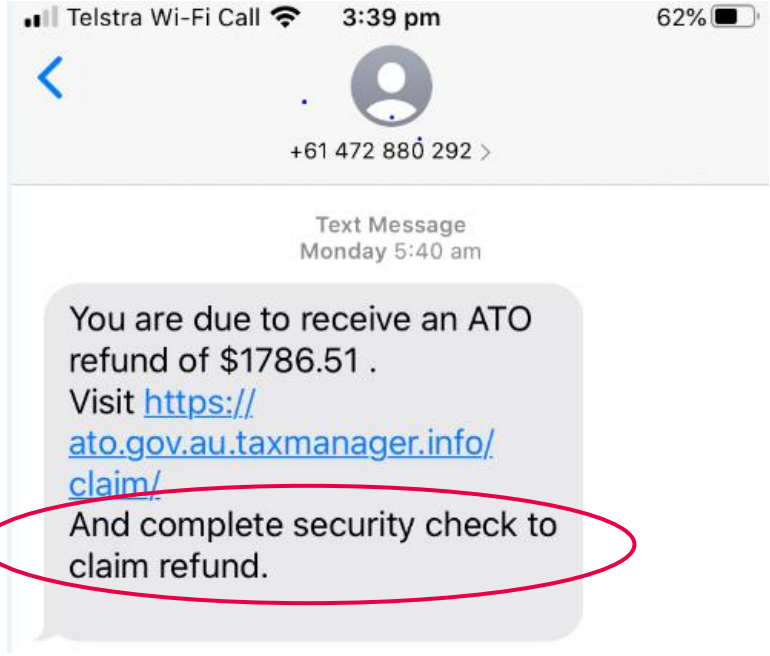


RSM

Smishing examples attempted on Roger, your presenter



Roger's response: "*That's great but I don't have a nab account!!!*"



Roger's response: "WTF (What The Fraud!) – No, I don't think so!!!"

Known occurring COVID-19 fraud and similar scams

- Scams to organise the early release of superannuation
- False vendors
  - e.g. some great tips in NSW ICAC's 'Managing Corrupt Conduct During the COVID-19 outbreak' (April 2020)
- Employees WFH (a risk to be aware of is considerable amount of the 'work time' being spent on non-employer related activities)
  - Ensure IT / cyber security measures are up-to-date like virus protection, firewalls, security patches etc. and follow your IT policy / advice
  - Be careful of security weaknesses (e.g. Zoom video conferencing security weakness - can expose Windows user names & passwords to attackers when malicious links are clicked in a chat window)
  - Watch what is in the background of your video conferencing (photos, identity documents, etc.)
  - Be wary for unidentified meeting participant(s)

The Entire ADF Has Been Banned From Using Zoom Meetings After Hamish Blake Showed Up In One

By Courtney Fry
06/04/2020

Share

THE AUSTRALIAN

The Australian Defence Force has told its personnel they're not to use Zoom meetings after **Hamish Blake** dropped in on an Air Force flight-log meeting last week, which didn't go down too well with the higher-ranking officers in the chat.

As per The Australian, all defence force staff and personnel were told to stop using the huge conferencing platform this morning due to apparent suspicions around security flaws in the conferencing system and fears that sensitive information could be accessed by unknown threat actors who exploit these flaws.

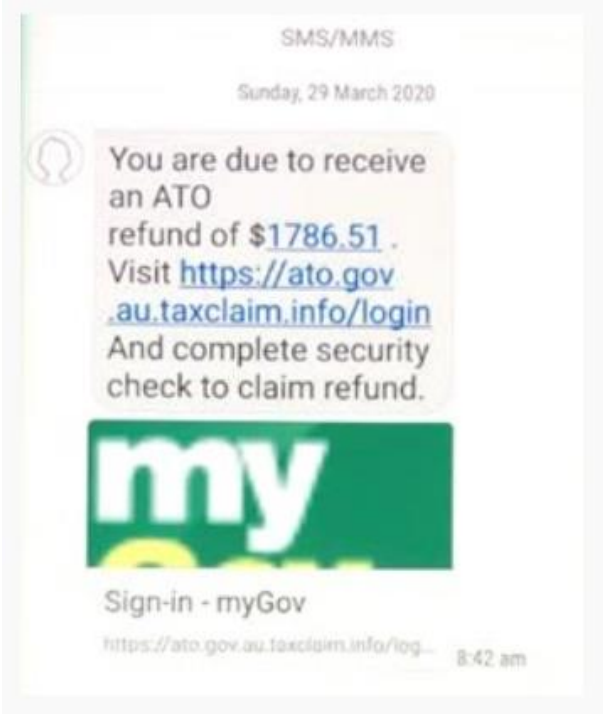
RSM

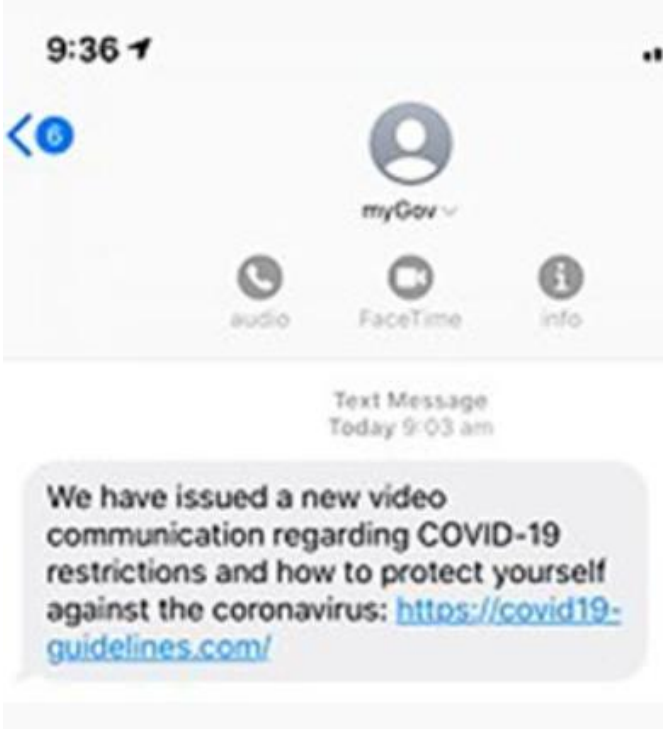
Known occurring COVID-19 fraud and similar scams

Phishing – Government impersonation scams

- Scammers are pretending to be government agencies providing information on COVID-19 through text messages and emails ‘phishing’ for your information. These contain malicious links and attachments designed to steal your personal and financial information.
- In the examples on the next slide the text messages appear to come from ‘GOV’ and ‘myGov’, with a malicious link to more information on COVID-19.

Fake myGov texts

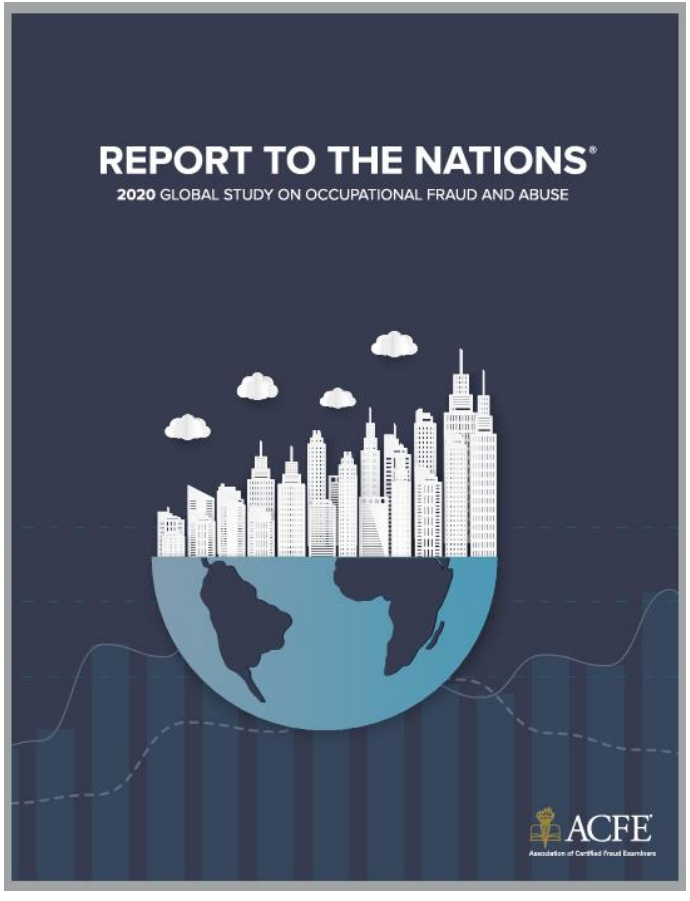


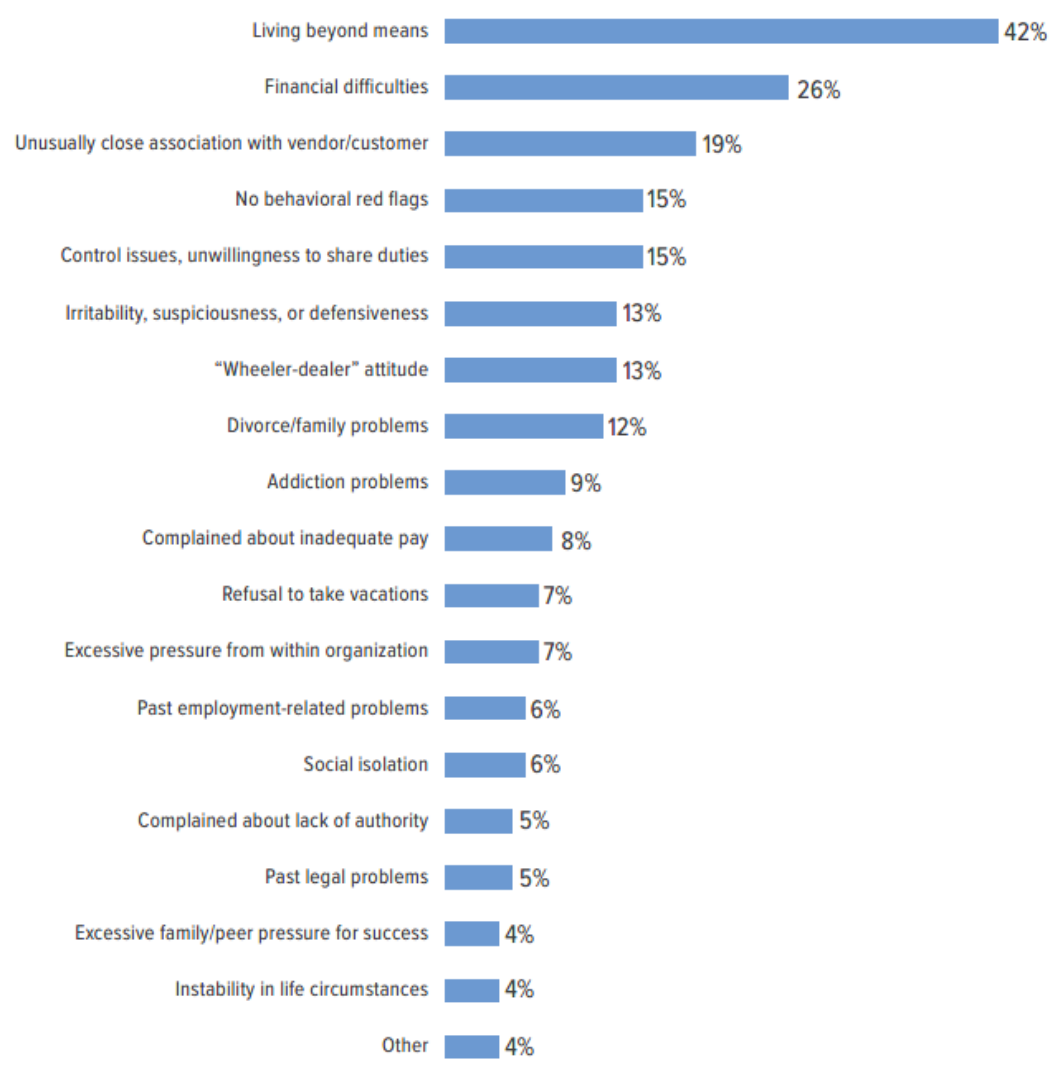


What we will cover

- Understand the various types of red flags and how these indicators can help detect fraudulent behaviour

Behavioural red flags





What can businesses do, including WFH risk mitigation

- Stay ever vigilant and diligent focussing on compliance, internal & external audit, & internal controls testing & strengthening
- Do not ignore or reduce your GRC requirements or practices
  - e.g. don't let your whistleblower program be ineffectual
- Provide employees with tips & traps of which to be aware to avoid being a victim personally of COVID-19 fraud scams, which translates to being more alert in daily work duties
- Consider conducting a COVID-19 anti-fraud/corruption and workplace misconduct review
- Do not forget about upskilling or continuous CPE development
  - e.g. CFE (Certified Fraud Examiner) Course

What we will cover

- **Ensuring conformance / compliance with various local and global fraud standards and legislation**

Australian Standard AS 8001-2008 Fraud & Corruption Control

AS 8001-2008 Fraud and corruption control

Section 2 Planning and Resourcing

- 2.1 Application
- 2.2 Fraud and corruption control planning
- 2.3 Review of the fraud and corruption control plan
- 2.4 Fraud and corruption control resources
- 2.5 Internal audit activity in the control of fraud and corruption

Section 3 Prevention

- 3.1 Application
- 3.2 Implementing and maintaining an integrity framework
- 3.3 Senior Management commitment to controlling the risks of fraud and corruption
- 3.4 Line management accountability
- 3.5 Internal control
- 3.6 Assessing fraud and corruption risk
- 3.7 Communication and awareness
- 3.8 Employment screening
- 3.9 Supplier and customer vetting
- 3.10 Controlling the risk of corruption

Section 4 Detection

- 4.1 Application
- 4.2 Implementing a fraud and corruption detection program
- 4.3 Role of the external auditor in detection of fraud
- 4.4 Avenues for reporting suspected incidents
- 4.5 Whistleblower protection program

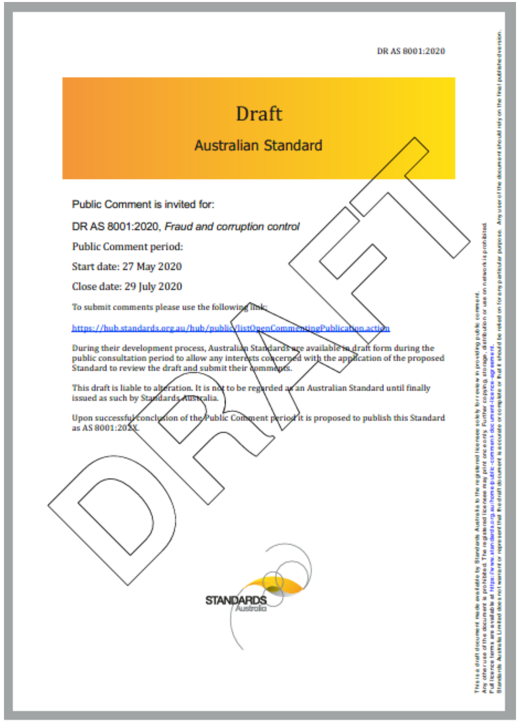
Section 5 Response

- 5.1 Application
- 5.2 Policies and procedures
- 5.3 Investigation
- 5.4 Internal reporting and escalation
- 5.5 Disciplinary procedures
- 5.6 External reporting
- 5.7 Civil action for recovery of losses
- 5.8 Review of internal controls
- 5.9 Insurance

RSM

Aust. Standard DR AS 8001:2020 Fraud and Corruption Control

1.4.14
fraud and corruption control system
FCCS
system for controlling the risks of fraud and corruption against or by an organization


DR AS 8001:2020

Draft
Australian Standard

Public Comment is invited for:

DR AS 8001:2020, *Fraud and corruption control*

Public Comment period:

Start date: 27 May 2020

Close date: 29 July 2020

To submit comments please use the following link:

https://hub.standards.org.au/hub/public/listOpenCommentingPublication.action

During their development process, Australian Standards are available in draft form during the public consultation period to allow any interests concerned with the application of the proposed Standard to review the draft and submit their comments.

This draft is liable to alteration. It is not to be regarded as an Australian Standard until finally issued as such by Standards Australia.

Upon successful conclusion of the Public Comment period it is proposed to publish this Standard as AS 8001:202X.

Aust. Standard DR AS 8001:2020 Fraud and Corruption Control

The terms "normative" and "informative" are used in Standards to define the application of the appendices to which they apply. A "normative" appendix is an integral part of a Standard, whereas an "informative" appendix is only for information and guidance.

1.3 Normative references

The following documents are referred to in the text in such a way that some or all of their content constitutes requirements of this document.

NOTE Documents for informative purposes are listed in the Bibliography.

AS 4811, *Employment screening*

AS ISO 31000, *Risk management — Guidelines*

AS ISO 37001, *Anti-bribery management systems — Requirements with guidance for use*

AS ISO/IEC 27001, *Information technology — Security techniques — Information security management systems — Requirements*

ISO/IEC 27037, *Information technology — Security techniques — Guidelines for identification, collection, acquisition and preservation of digital evidence*

ISO/IEC 27041, *Information technology — Security techniques – Guidance on assuring suitability and adequacy of event investigative method*

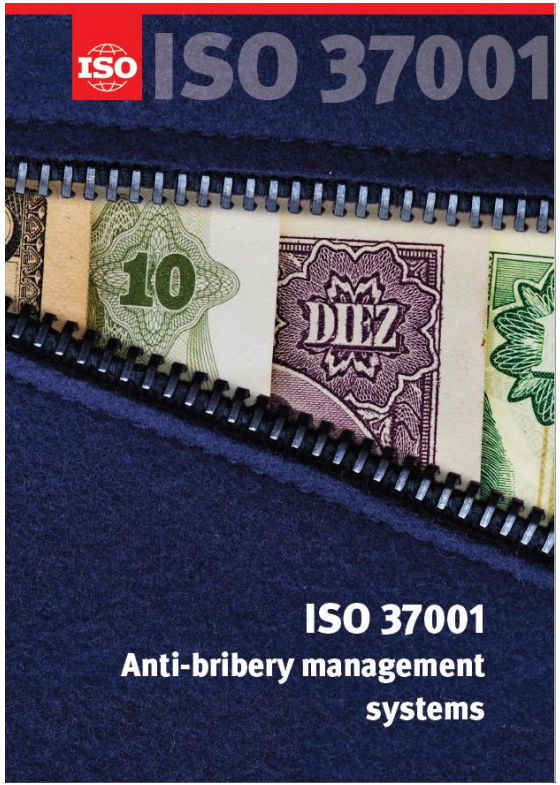
ISO/IEC 27042, *Information technology — Security techniques – Guidelines for the analysis and interpretation of digital evidence*

ISO/IEC 27043, *Information technology — Security techniques - Incident investigation principles and processes*

NIST SP 800-61R2, *Incident handling*

RSM

ISO 37001 Anti-bribery management systems 2016



"Reasonable and proportionate"

Controls:

1. Bribery risk assessment
2. Tone from the top
3. Anti-bribery compliance function
4. Employment (due diligence, performance bonuses, conflicts of interest)
5. Awareness and training
6. Due diligence
7. Financial controls
8. Non-financial controls

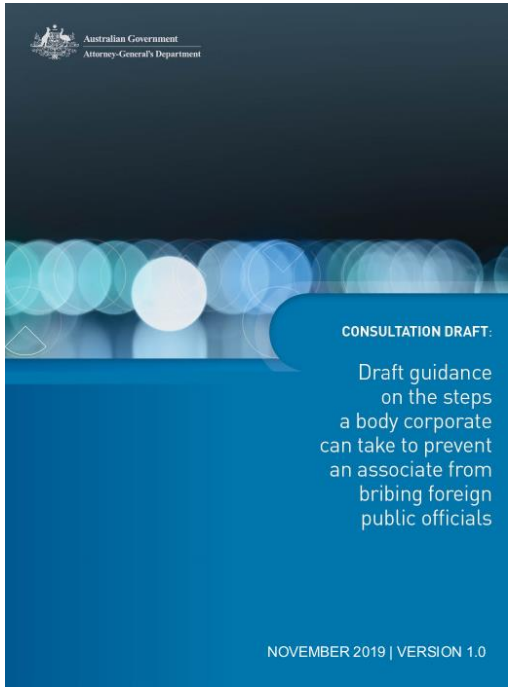
RSM

ISO 37001 Anti-bribery management systems 2016

51. The Crimes Legislation Amendment (Combatting Corporate Crime) Bill 2019 proposes a new corporate offence of failing to prevent foreign bribery. This offence would automatically trigger the liability of a corporation where an associate of the corporation commits a foreign bribery offence, under section 70.2 of the Criminal Code, for the profit or gain of the corporation.

52. However, the offence would not apply if the corporation has adequate procedures in place designed to prevent its associates from committing foreign bribery (guidance on the types of measures that may constitute 'adequate procedures' is set out in Part 2 of this document).

53. A similar offence has been successfully implemented in the United Kingdom and has reportedly had a significant positive influence on the adoption of effective corporate compliance programs to prevent bribery.



Adequate procedures (principles based rather than a checklist):

1. Risk assessment
2. Management dedication
3. Due diligence
4. Communication and training
5. Confidential whistleblowing reporting mechanisms (and investigation)
6. Monitoring and review of compliance programs

What we will cover

- Identifying current high-risk fraud areas

A fraud classification tree

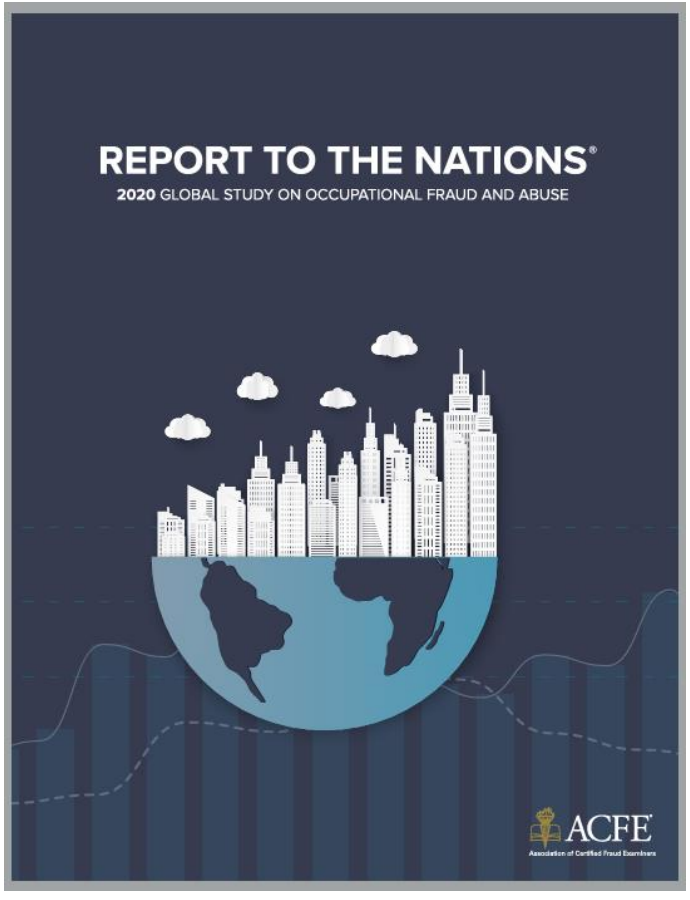
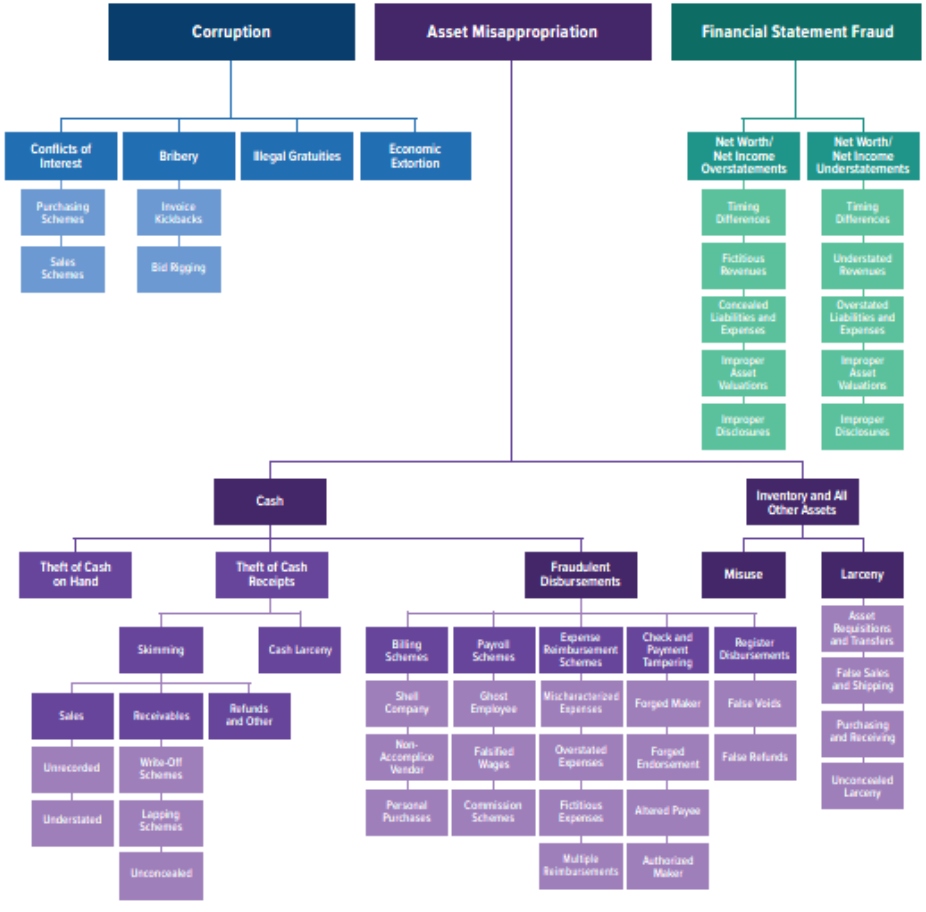


FIG. 3 **Occupational Fraud and Abuse Classification System (the Fraud Tree)**[1]



[1] The definitions for many of the categories of fraud schemes in the *Fraud Tree* are found in the Glossary of Terminology on pg. 86.

What we will cover

- Determining methods to strengthen your organisation's fraud control framework

ACFE's Anti-Fraud Playbook 2020

- Rigorously implement better practice guide(s)
- Comply with legislation:
  - Whistleblowers
  - Foreign bribery and corruption
  - Modern slavery legislation
  - Etc.

ACFE's Anti-Fraud Playbook 2020

FIG. 2 Enterprise Anti-Fraud Maturity Assessment Model©

	AD HOC LEVEL ONE	INITIAL LEVEL TWO	REPEATABLE LEVEL THREE	MANAGED LEVEL FOUR	LEADERSHIP LEVEL FIVE
FRAUD RISK GOVERNANCE	• Undocumented and in a state of dynamic change, tending to be driven in an ad hoc, uncontrolled, and reactive manner by users or events • Fraud risk management processes are disorganized, even chaotic • Success is likely to depend on individual efforts, and is not considered to be repeatable because processes would not be sufficiently defined and documented to allow them to be replicated	• The organization is aware of the need for a more formal fraud risk management approach • Processes are repeatable, possibly with consistent results • Fraud risk definitions often vary across the organization. Fraud risk is assessed and/or managed in silos, and enterprise-wide risks are not routinely considered • Risks are managed largely in a reactive way	• There are sets of defined and documented standard processes established. Approaches are standardized and repeatable. • Fraud risk management is aligned with the organization's external and internal environment and integrates with the organization's enterprise risk program • Senior levels and the board of directors receive fraud risk overviews or reports • Roles, responsibilities, and performance measurements are defined and documented	• Fraud risk management activities across the organization are aligned with controls and performance indicators • Performance and quality are defined and can be measured • Information on fraud risks is aggregated and analyzed and is easily available to management. A process for notifying management in changes to fraud risk profiles is established and operating • Full integration of the fraud risk principles into management processes has been achieved	• The organization's focus is on continually improving fraud risk management through both incremental and innovative changes/improvements • Management discusses fraud risk with a goal of strategic, operational, and profitability improvements • Fraud risk tolerance has been established and fraud risk assessments are designed to inform the board and management when thresholds have been exceeded • Organization consistently performs ongoing and ad hoc monitoring of its antifraud controls and process, and has an established reporting structure in place
FRAUD RISK ASSESSMENT					
FRAUD CONTROL ACTIVITIES					
FRAUD INVESTIGATION & CORRECTIVE ACTION					
FRAUD MONITORING ACTIVITIES					

RSM

Anti-fraud training / global CFE certification

RSM is the exclusive Authorised Trainers in Australia for the global ACFE (Association of Certified Fraud Examiner) CFE (Certified Fraud Examiners) Exam Review Course – now virtual until in-person can be re-instated

- Investigation
- Law
- Financial Transactions and Fraud Schemes
- Fraud Prevention and Deterrence

What we will cover

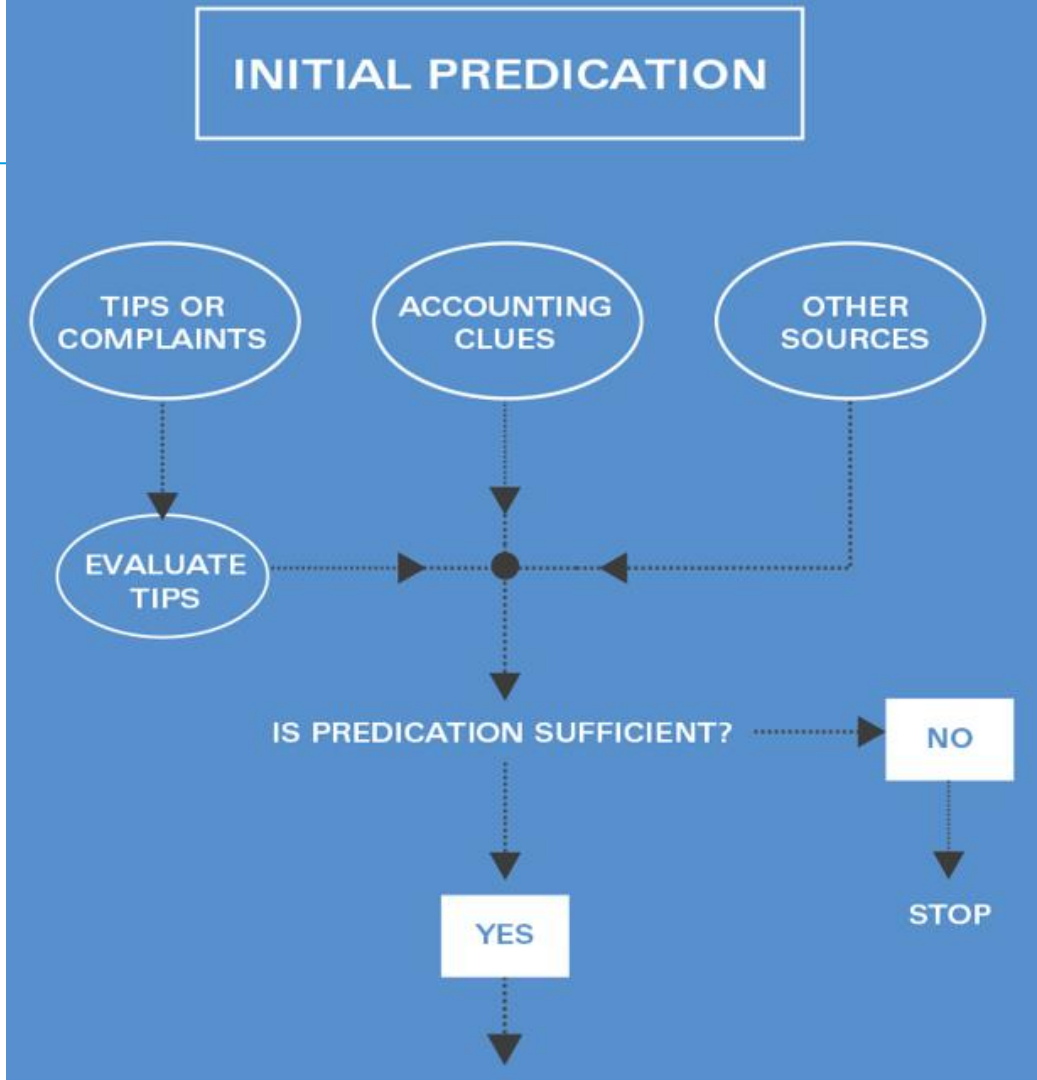
- Procedure to undertake when fraud is uncovered

Adapted from ACFE's Anti-Fraud Playbook 2020

Typical components and factors to consider for investigations:

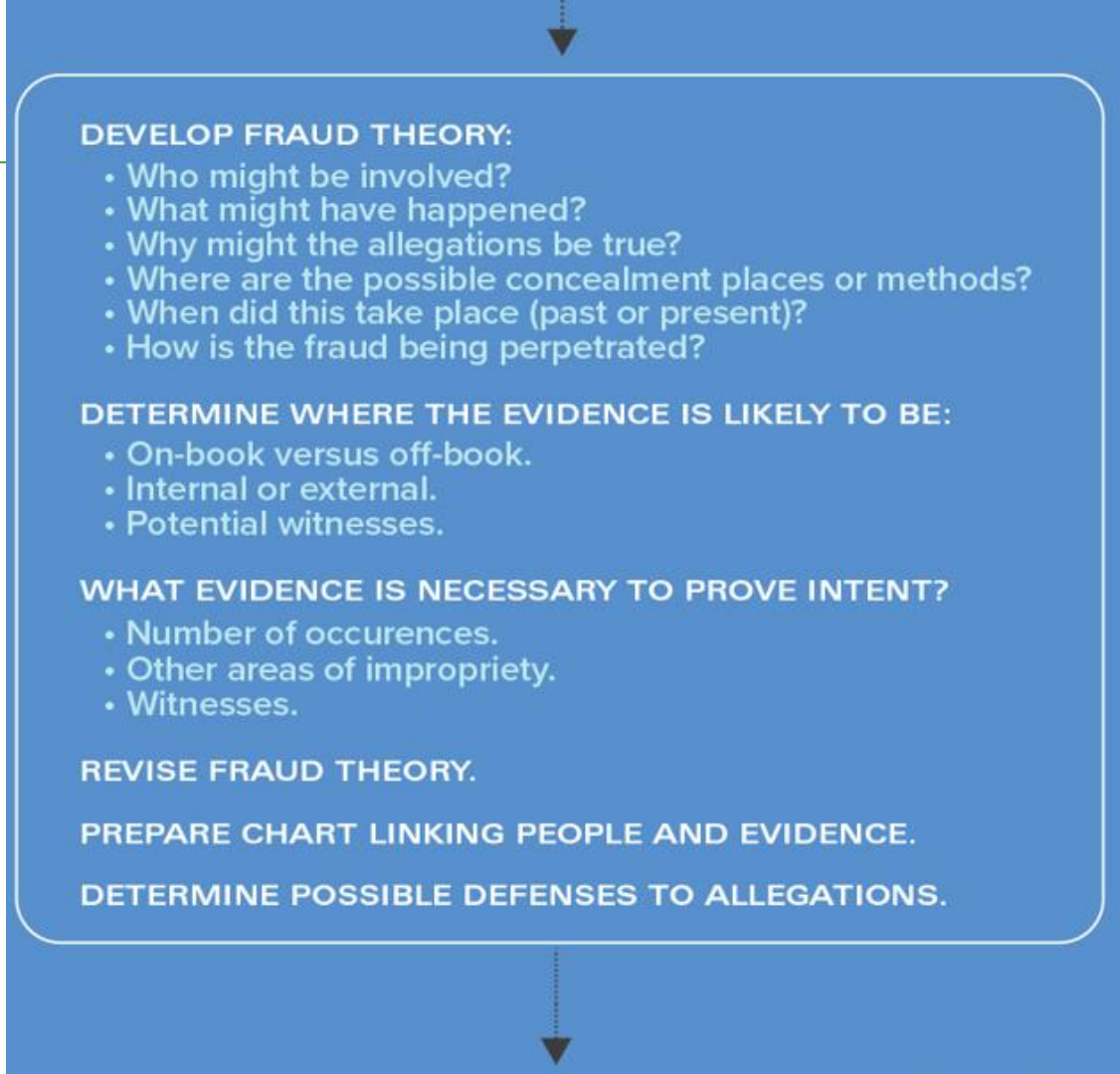
Investigation components	Some steps to consider (varies with each investigation and its type)
Evidence gathering (multiple sources)	Time sensitivity
Computer forensics	Confidentiality
Develop and test hypotheses	Legal privilege
Gather external records	Objectivity
Interviewing – witnesses and POIs	'Whistleblower' / witness management
Perform data analysis	Professional scepticism

ACFE's Fraud-Theory Approach



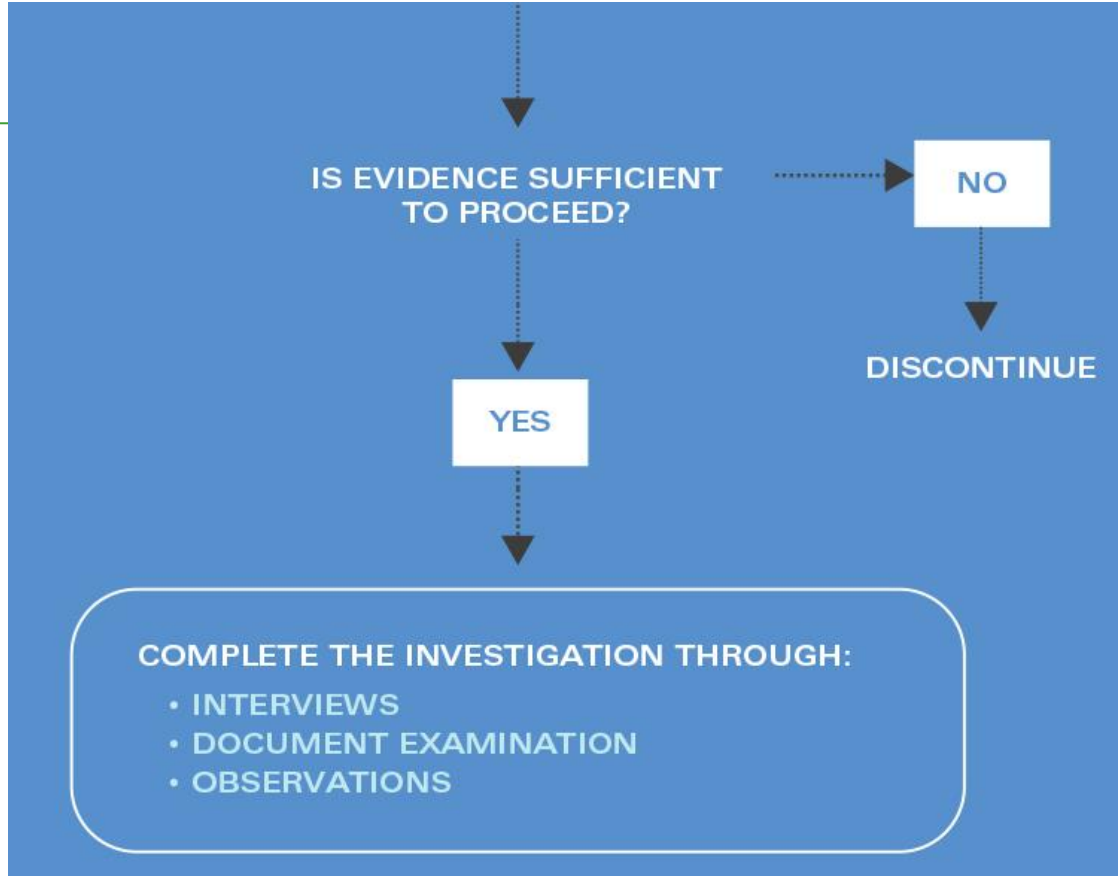
[Source: ACFE Fraud Magazine article 'Learning the Art of Fraud Examination' by Dick Carozza CFE, a publication of the Association of Certified Fraud Examiners, Vol. 34, No. 6, November/December 2019, https://www.acfe.com/article.aspx?id=4295009021]

ACFE's Fraud-Theory Approach



[Source: ACFE Fraud Magazine article 'Learning the Art of Fraud Examination' by Dick Carozza CFE, a publication of the Association of Certified Fraud Examiners, Vol. 34, No. 6, November/December 2019, https://www.acfe.com/article.aspx?id=4295009021]

ACFE's Fraud-Theory Approach



[Source: ACFE Fraud Magazine article 'Learning the Art of Fraud Examination' by Dick Carozza CFE, a publication of the Association of Certified Fraud Examiners, Vol. 34, No. 6, November/December 2019, https://www.acfe.com/article.aspx?id=4295009021]

Disclaimer

This presentation is intended as general information only and should not be considered as advice on any matter and should not be relied upon as such. The information in this presentation has been prepared without taking into account any individual objectives, financial situation or needs. No member of RSM Australia, no any of their employees or directors gives any warranty of accuracy or reliability nor accepts any liability in any other way including by reason of negligence for any errors or omissions contained in the presentation, to the extent permitted by law.

Liability limited by a scheme approved under Professional Standards legislation.

Questions and answers?