Fraud and the COVID-19 Stimulus Package

Advice for public officials

APRIL 2020

Office of the Independent Commissioner Against Corruption NT

Where the public sector is responsible for leading emergency management, there is an expectation that the government will play a role in controlling broader fraud.[1]

[1] Fraud in Emergency Management & Recovery (2020), International Public Sector Fraud Forum, p 11.

Contents

Introduction

The Northern Territory Government has introduced over $300 million in stimulus programs to support Territorians and Territory businesses during the economic downturn associated with the COVID-19 pandemic.

While the stimulus package is designed to help those who need it most, it also creates a risk of improper conduct. Improper conduct includes corrupt conduct, misconduct and anti-democratic conduct. It also includes fraud. In Australia, recent examples of fraud include the Indigenous Employment Provisional Sum and the emergence of fake fundraising organisations following the 2019-2020 summer bushfires.

Making sure that stimulus program benefits are maximised is important, but particularly so when the Northern Territory Government is looking to find savings and maximise value under its Plan for Budget Repair.

'Phishing' gives rise to an increased risk of identity theft to facilitate fraudulent activity. ActionFraud[2] (UK) reported that coronavirus-related scams, including phishing attacks, increased by 400% in March 2020. Scamwatch[3] (Australia) has issued warnings about scams related to the Australian Government's Household Stimulus package. Northern Territory Police confirmed that online fraud is increasing and warned that sophisticated cyber criminals are involved.[4]

Agencies dealing with stimulus programs are urged to be vigilant to potential fraud and ensure people attempting to defraud the Northern Territory taxpayer are stopped and referred to the police. All public officers have an obligation to report, where appropriate, to the office of the Independent Commissioner Against Corruption (ICAC).

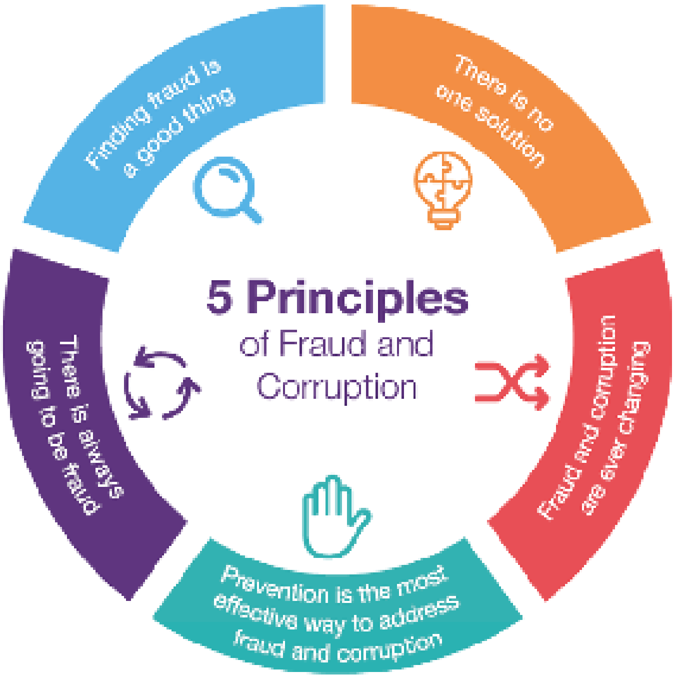
The advent of COVID-19 has resulted in a change to normal work practices, with a significant number of people working from home. This will have an impact on the way public sector functions are performed, and there is a need to adapt service delivery while maintaining the integrity and values of the Northern Territory public sector.

This guide is intended to alert public officers to the potential for fraud and improper conduct during a time of uncertainty, changing business practices and the unprecedented flow of public monies designed for economic stimulus to reach those most in need.

[2] https://www.bedfordshire.police.uk/news-and-appeals/corona-fraud-warning-march20
[3] https://www.scamwatch.gov.au/news/australian-government-stimulus-package-scams
[4] Media release, 3 April 2020.

Principles of fraud control in emergency management

The International Public Sector Fraud forum is comprised of representatives from Australia, Canada, New Zealand, the United Kingdom and the United States. The forum has identified five principles for public sector fraud:[5]


5 Principles
of Fraud and
Corruption
Finding fraud is a good thing
There is no one solution
Fraud and corruption are ever changing
Prevention is the most effective way to address fraud and corruption
There is always going to be fraud

Preventing fraud through effective counter fraud practices reduces loss and reputation damage. It also requires fewer resources than an approach focused on detection and recovery.

Note that here, the word 'fraud' is used to cover economic crime generally (that is, individuals or groups being dishonest for their own gain) and can include loss as a result of corruption, where corruption leads to fraud.

[5] Fraud in Emergency Management & Recovery (2020), International Public Sector Fraud Forum, 5.

Preparation: what to expect

Accept that there is an inherently high risk of fraud, and that it is very likely to happen

Plan for fraud monitoring and spot checking, and **record** the steps that you take to develop and implement the process

Integrate fraud control resources (personnel) into the policy and process design **to build awareness of fraud risks**

The business and fraud control resources should work together to **implement low friction counter-measures** to prevent fraud risk where possible

Carry out **targeted post-event assurance** to look for fraud, and ensure access to fraud investigation resources

Be **mindful of the shift** from emergency payments into longer term services and revisit the control framework – especially where large sums are invested

Be mindful that the fundamental purpose in an emergency context is **getting payments and services to those in need**.

Corrupt conduct and disaster relief

Examples of fraudulent conduct following disasters include:

- More than 400 bushfire fundraiser scams were reported to ScamWatch during the 2019-2020 bushfires in Australia. The reports were so extensive the Australian Competition and Consumer Commission set up a dedicated hotline just to report bushfire scams.
- Following the Grenfell Tower fire in 2017 an individual falsely claimed over £95 000 of government support by fraudulently claiming he was sleeping in the building at the time of the fire.
- Shortly after Hurricane Katrina in 2005, Scott Benson and Chris Armstrong masqueraded as Salvation Army workers to con more than 2500 police officers, firefighters, sheriff's deputies and FBI agents into disclosing personal information. The men told officers that they were eligible for debit vouchers worth $5000 in a program sponsored by media company Viacom. The men were charged with false impersonation and conspiracy to commit identity theft.
- A Federal Emergency Management Agency (FEMA) inspector was arrested on charges of accepting kickbacks for approving false hurricane damage claims.
- A former FEMA manager was indicted for embezzlement of a caravan intended for victims of Hurricanes Katrina and Rita. The man took the caravan and his government-owned motor vehicle for personal use and was further charged with attempting to corruptly influence the investigation into his conduct.
- Eight defendants were sentenced in 2008 for conspiracy to defraud FEMA. The conduct involved more than 70 applications for Hurricanes Katrina and Rita relief benefits on behalf of residents who were not victims of the hurricanes. Those involved faced a number of penalties, including imprisonment for 33 months and an order for restitution of $92 958 for the leader.[6]

The International Public Sector Fraud Forum noted: 'Where the public sector is responsible for leading emergency management, there is an expectation that the government will play a role in controlling broader fraud.'[7]

In these situations, public officers are responding to government decisions made at short notice with the principal goal of getting money to those who need it the most. The rapidly changing environment in which these decisions are made and programs delivered represents a departure from established controls and processes, and therefore increased risk. A risk management map dealing with the progression of a stimulus rollout and associated risks appears on page 9.

Price gouging

When disaster strikes, whether it is a cyclone, flood or pandemic, consumers can react by panic-buying or stock-piling basic goods. When retailers take advantage of these spikes in demand—which are often coupled with supply shortages—by charging exorbitant prices for necessities, it is referred to as 'price gouging'.

In the case of government stimulus packages such as the Northern Territory Government's $30 million Home Improvement Scheme, some suppliers may be tempted to inflate prices to take unfair advantage of government efforts to maintain economic activity during the COVID-19 downturn.

[6] Fraud in Emergency Management & Recovery (2020), International Public Sector Fraud Forum, p 20.
[7] Fraud in Emergency Management & Recovery (2020), International Public Sector Fraud Forum, p 11.

Price gouging during a time of emergency is considered unconscionable conduct.[8]

Unconscionable conduct is particularly harsh or oppressive. It may also be where one party knowingly exploits the special disadvantage of another. It needs to be more than just hard commercial bargaining; it must be against conscience as judged against the norms of society. Australian courts have found transactions or dealings to be unconscionable when they are deliberate, involve serious misconduct or are clearly unfair and unreasonable.[9]

Under this federal law, the penalties for unconscionable conduct are:

For a corporation, the greater of:

- $10 million; OR
- three times the value of the benefit received; OR
- where the benefit cannot be calculated, 10 per cent of annual turnover in the preceding 12 months.

For an individual:

- $500 000 per breach.[10]

Conduct of this nature constitutes improper conduct under the ICAC Act. It includes corrupt conduct, misconduct, unsatisfactory conduct, and secondary conduct including attempt, complicity, incitement and conspiracy.

Cartels and collusive tendering

Collusion, also known as price fixing, is illegal. Collusion occurs when competitors work together to fix prices rather than compete against each other. This conduct restricts competition, increases prices and restricts consumer choice.

Indications of price fixing can include:

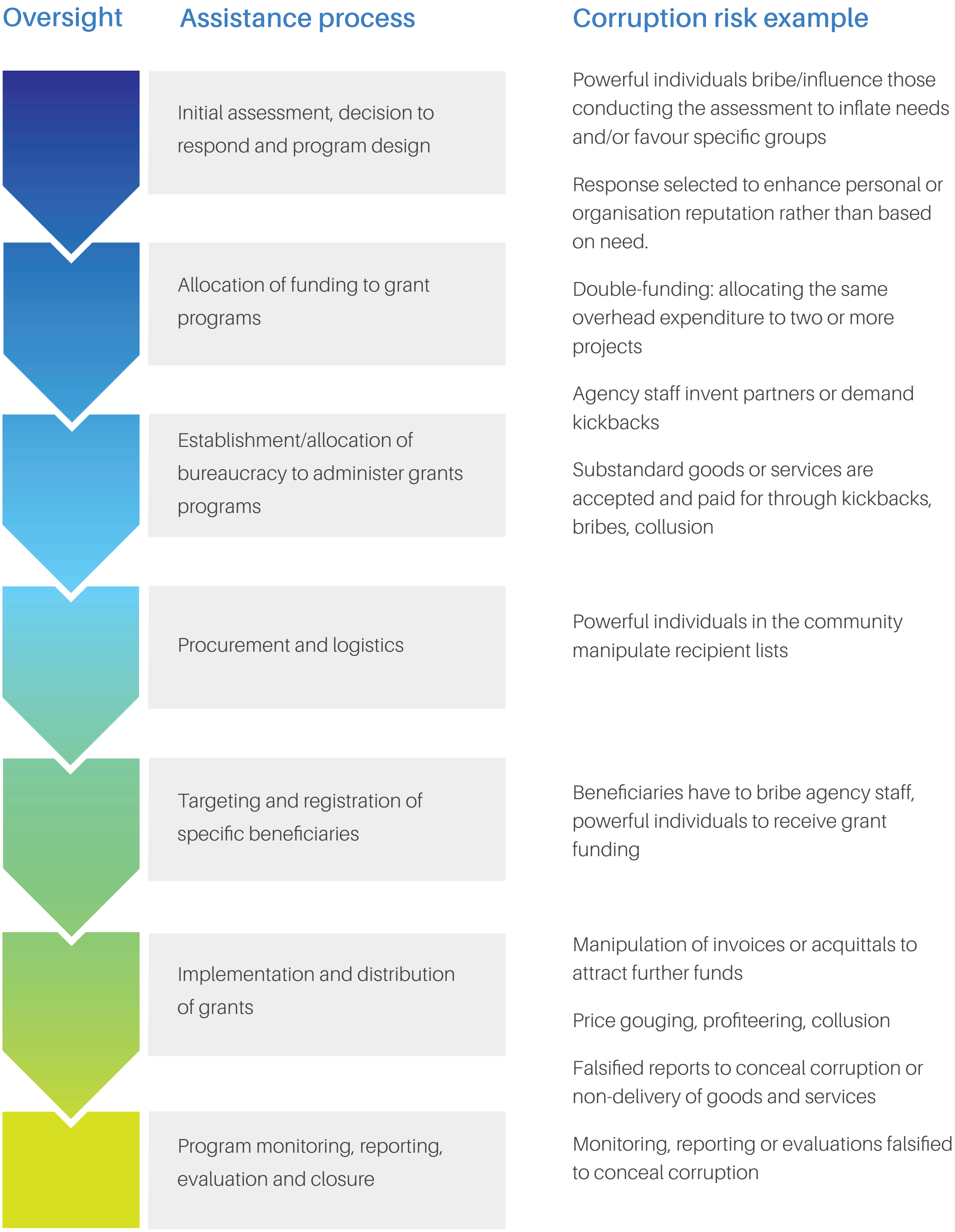
- quotes that are much higher than expected. This may indicate collusive pricing
- all suppliers raise prices simultaneously and beyond what seems to be justified
- prices submitted are much higher than previous quotes or published price lists
- quotes are missing detailed 'workings' to show how the price was calculated
- a new supplier's price is lower than the usual businesses quoting
- prices drop markedly after a new supplier quotes.[11]

Lying about the reason for price gouging is also illegal. If suppliers fabricate the reasons for inflated price rises, that is a violation of Australian Consumer Law.[12]

By engaging in profiteering, price gouging or collusion–quite apart from it being illegal–suppliers are unfairly and unreasonably wasting government funds intended to help people and businesses across the Territory in a time of crisis.

[8] See sections 20 and 21 of the Competition and Consumer Act 2010 (Cth).
[9] https://www.accc.gov.au/system/files/482_Business%20Snapshot_Unconscionable%20conduct_FA2.pdf
[10] Queensland Government, Fair Trading https://www.qld.gov.au/law/laws-regulated-industries-and-accountability/queensland-laws-and-regulations/fair-trading-services-programs-and-resources/fair-trading-latest-news/disaster-assistance/profiteering-price-gouging
[11] Australian Competition & Consumer Commission https://www.accc.gov.au/business/anti-competitive-behaviour/cartels/price-fixing
[12] ACCC quoted by Choice https://www.choice.com.au/shopping/online-shopping/selling-online/articles/coronavirus-and-price-gouging
[13] https://www.accc.gov.au/media-release/alice-springs-car-rental-price-fix-costs-companies-and-managers-15-million

Mapping risk for stimulus grants[13]



Oversight

Assistance process

- Initial assessment, decision to respond and program design
- Allocation of funding to grant programs
- Establishment/allocation of bureaucracy to administer grants programs
- Procurement and logistics
- Targeting and registration of specific beneficiaries
- Implementation and distribution of grants
- Program monitoring, reporting, evaluation and closure

Corruption risk example

Powerful individuals bribe/influence those conducting the assessment to inflate needs and/or favour specific groups

Response selected to enhance personal or organisation reputation rather than based on need.

Double-funding: allocating the same overhead expenditure to two or more projects

Agency staff invent partners or demand kickbacks

Substandard goods or services are accepted and paid for through kickbacks, bribes, collusion

Powerful individuals in the community manipulate recipient lists

Beneficiaries have to bribe agency staff, powerful individuals to receive grant funding

Manipulation of invoices or acquittals to attract further funds

Price gouging, profiteering, collusion

Falsified reports to conceal corruption or non-delivery of goods and services

Monitoring, reporting or evaluations falsified to conceal corruption

[13] Adapted from Ewins, P et al (2006) Mapping the Risks of Corruption in Humanitarian Action.

Managing fraud risk

Agencies should have risk management teams in place to identify and assess the risks specific to the programs they administer. Risk management plans should include rolling or spot audits and grant acquittal processes.

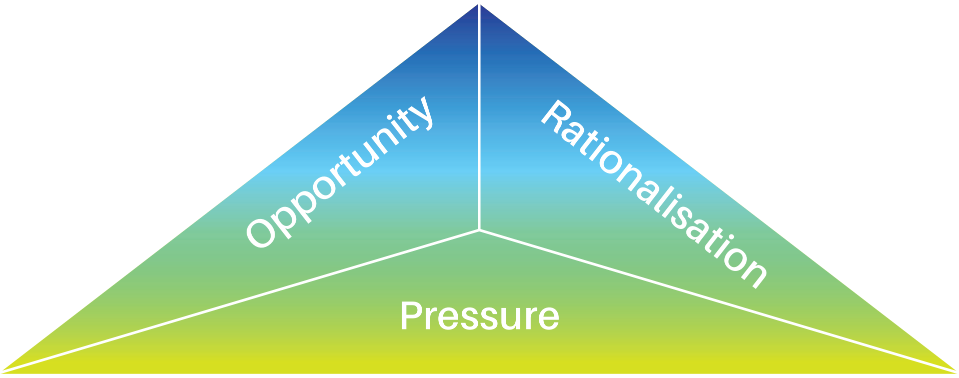
More broadly, agencies should be alert to:

- the need to cross-check and verify business or company registration numbers
- the need to confirm that the business meets the criteria of grant eligibility and does trade in the Northern Territory
- companies operating in several locations across Australia that make repeated claims using the same or different ABNs or other individual identifiers
- check that the ABN or ACN do not belong to an employee of the agency
- individuals or business entities attempting to bribe public officers for preferential treatment
- fraudulent claims from individuals claiming to be the proprietors of a small business
- multiple Home Improvement Scheme grant applications by the owner of several properties
- price gouging by suppliers engaged to perform works for grant recipients
- individuals falsely claiming to be counsellors or psychologists
- individuals falsely claiming to be financial advisors or counsellors
- individuals claiming to provide crisis accommodation
- price gouging by crisis accommodation providers
- fraudulent paperwork in relation to valid legal entity status
- inflation of employee numbers required to complete work
- incomplete or unfinished work claimed as completed
- incomplete provision of details, which may indicate identity theft
- home-based business operators claiming against funds intended for hospitality venues (restaurants, hotels, etc).

Using established providers where possible can often be a lower risk option than using unestablished and untested providers about whom agencies have less information. However, it is individuals who commit fraud, not organisations. It is not possible, therefore, to eliminate the risk of fraud simply by using established and 'trusted' providers.

Corruption trends during economic downturns

Evidence indicates that some forms of corruption and serious misconduct become more prevalent during periods of significant disruption and economic downturn.



The fraud triangle[14] tells us that a combination of financial pressure, opportunity and rationalisation is conducive to fraud. The COVID-19 pandemic and related economic downturn have intensified all three points of the triangle.

1. Financial pressure

Employees, suppliers and customers (and their families) may be experiencing actual or anticipated financial hardship (for example, a public servant's spouse loses their job, a supplier's work dries up, superannuation or other investments lose a large proportion of their value, or a public official becomes concerned about being made redundant).

2. Opportunity

Agencies controls and normal levels of supervision may weaken or cease to function (for example, normal segregation of duties may not be in place or IT systems may not be accessible, multi-agency teams may be formed, social distancing practices and people working from home).

3. Rationalisation

Perpetrators may find it easier to rationalise dishonest behaviour (for example, individuals may find it morally justifiable to engage in fraud if it is in response to acute circumstances, or if they perceive others getting away with it).

In addition, fraud and corruption risks may arise externally at specific points in the supply chain.

For an unknown period of time, agency operations will not be on a business-as-usual footing. However, agencies that can move their control environment back to business-as-usual quickly will lower the chances of corrupt conduct. Once this happens, it may be useful to direct audit activities towards identifying suspicious anomalies or exceptions that emerged during the pandemic.

[14] See generally Transparency International.

Risks associated with working from home

Working from home results in a loss of manager-employee and peer-to-peer interaction that normally takes place in an office environment. However there are a number of ways to address the risks of leaving employees isolated or without the necessary or normal interaction to perform their duties.

Bearing in mind the risks associated with cybersecurity, technology meetings and staff interaction can be held via teleconference or video conference.[15] Confidentiality of material should be maintained in the home environment by prohibiting access by family members to the NTG VPN. Similarly, documents should not be left on a home printer or scanner. Agency IT equipment allocated to staff working from home should be recorded and, if necessary, protocols should be established for the use of electronic signatures.

Risks associated with cyber fraud and online hoaxes

As noted earlier, reports of COVID-19-related cyber fraud have already begun to emerge. See, for instance, advice published by the Australian Competition and Consumer Commission[16] and the Australian Cyber Security Centre[17]. Northern Territory Police have issued a warning about the increase in cyberfraud, much of which uses a social engineering approach. That is, the frauds involve impersonating a trusted person, such as a senior manager or an officer from the organisation’s IT department. In an environment where many staff are working from home and normal face-to-face interactions are limited, socially engineered cyber frauds are more likely to succeed. In addition, the COVID-19 pandemic has prompted a number of criminals to impersonate government agencies as part of an attempt to defraud citizens.

It is recommended that agencies observe the following practices:

- in the first instance, assume that any request to change a supplier’s or employee’s bank account number could be an attempted fraud (verify the request by telephoning the relevant supplier/employee, without relying on the contact information contained in a potentially false email message)
- be wary of adding new suppliers to the vendor master file, especially if they are not already on a pre-qualified panel or if they have invoiced the agency without being issued a purchase order
- direct accounts payable staff to challenge any suspicious requests for payment, even if it purports to come from a senior manager or the agency head
- do not pay invoices without performing a three-way match
- alert customers and citizens to attempts by third parties to impersonate the agency or its staff
- remind staff not to open emails, or attachments or click on links from untrustworthy sources.[18]

[15] Note that recent security enhancements to Zoom apply automatically only to educational institutions and anyone using the application privately must alter the privacy settings themselves.
[16] COVID-19 (coronavirus) scams, 18 March 2020
[17] Threat update: COVID-19 malicious cyber activity, 27 March 2020
[18] Adapted from Managing corrupt conduct during the COVID-19 outbreak (April 2020), NSW ICAC

Maintaining public sector values and ethics

Agencies should have a fraud and corruption control program. Given the current circumstances, it is reasonable to expect that elements of those programs will need to be put on hold or modified. Communication, therefore, is the key to reminding staff of their obligations, encouraging people to report fraud, and welcoming robust advice in relation to suspected fraud.

It is a good time to revisit and refresh **Conflict of Interest** training and declarations, especially for those involved in administering the stimulus programs.

Conflicts of interest in public officers does not necessarily or normally constitute corrupt conduct. However, corrupt conduct can arise when a conflict of interest is concealed, understated, mismanaged or abused.

Public officers' responsibilities for declaring conflicts of interest (whether perceived, potential or actual) are set out in the Northern Territory Government's Employment Instruction Number 12 – Code of Conduct.

Freecall
1800 250 918

Level 7, 9-11 Cavenagh Street
Darwin NT 0801
GPO Box 3750 Darwin NT 0801

icac.nt.gov.au

Office of the
Independent
Commissioner
Against
Corruption NT