International Public Sector Fraud Forum
Bringing countries together to fight public sector fraud

International Public Sector Fraud Forum

Guide to Understanding the Total Impact of Fraud

February 2020

Cabinet Office

Commonwealth Fraud Prevention Centre

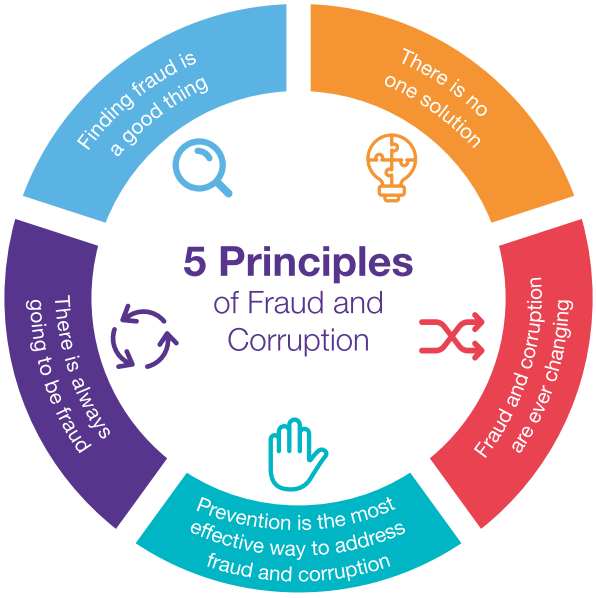
Produced in collaboration with the Cabinet Office and the Commonwealth Fraud Prevention Centre.

Contents

The International Public Sector Fraud Forum

The International Public Sector Fraud Forum (IPSFF) currently consists of representatives from organisations in the governments of Australia, Canada, New Zealand, the United Kingdom and the United States. The collective aim of the Forum is to come together to share best and leading practice in fraud management and control across public borders.

The Forum has established 5 principles for public sector fraud.



1. There is always going to be fraud

It is a fact that some individuals will look to make gains where there is opportunity, and organisations need robust processes in place to prevent, detect and respond to fraud and corruption.

2. Finding fraud is a good thing

If you don't find fraud you can't fight it. This requires a change in perspective so the identification of fraud is viewed as a positive and proactive achievement.

3. There is no one solution

Addressing fraud needs a holistic response incorporating detection, prevention and redress, underpinned by a strong understanding of risk. It also requires cooperation between organisations under a spirit of collaboration.

4. Fraud and corruption are ever changing

Fraud, and counter fraud practices, evolve very quickly and organisations must be agile and change their approach to deal with these evolutions.

5. Prevention is the most effective way to address fraud and corruption

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

Executive summary

Fraud is a serious, underestimated and unchecked problem. Every public body is an active target for fraudsters. Unfortunately, public bodies do not always consider fraud when conducting their activities. Even when fraud is considered, public bodies can find it difficult to define, measure and articulate the problem without guidance. In addition, the focus can be too centred on financial loss. In reality, the impact of fraud goes well beyond this.

Fraud impacts on people, industries, public bodies, services and the environment and all of these can be irreversibly harmed. Understanding the total impact of fraud and not just the financial loss allows public bodies to make better informed decisions.

Serious impacts can arise from any type of fraud, whether it's perpetrated by opportunistic individuals or serious and organised crime groups. However, serious and organised crime can often amplify the scale and impacts of fraud, and professional facilitators make their activities more difficult to detect and uproot.

This guide sets out the key extending impacts of fraud, noting that many cases of fraud will have a number of different impacts. It also builds a case for investing in counter fraud measures by explaining the comprehensive impact of fraud. Understanding these impacts enables public bodies to prevent or mitigate these impacts and educate their employees and stakeholders on the importance of counter fraud measures.

The impacts of fraud set out in this guide are:

Human impact

Fraud against public bodies is not a victimless crime. Fraud can be a traumatic experience that often causes real and irreversible impacts for victims, their families, carers and communities. Those who rely on government services, such as the elderly, the vulnerable, the sick and the disadvantaged, are often the ones most harmed directly or indirectly by fraud. Fraud can have a devastating and compounding effect on these victims; amplifying the disadvantage, vulnerability and inequality they suffer. Fraud can also cause lasting mental and physical trauma for victims, and in some cases, take people's lives.

Government outcomes impact

Fraud against public bodies compromises the government's ability to deliver services and achieve intended outcomes. Money and services are diverted away from the intended targets and the services delivered can be substandard or unsafe. This can lead to program failure. It also leads to lost opportunities for individuals and businesses.

Reputational impact

Fraud happens and can affect any public body. However, when it is handled poorly, fraud against government programs can result in an erosion of trust in government and industries, and lead to a loss of international and economic reputation. This is particularly true when fraud is facilitated by corruption.

Government system impact

Fraud drains government resources across multiple areas including investigations and compliance, prosecution, prison, welfare, identification and computer systems.

Industry impact

Fraud against public bodies can result in distorted markets where fraudsters obtain a competitive advantage and drive legitimate business out. It can affect services delivered by business and expose other sectors to further instances of fraud. It can also result in greater burdens on charities and community services who assist those affected by fraud against public bodies.

Environmental impact

Fraud against public bodies can lead to immediate and long term environmental damage through pollution and damaging ecosystems and biodiversity. It can also result in significant clean-up costs.

Security impact

Fraud against public bodies can compromise national defence and security, putting service men and women, and citizens at risk. It can also damage international standing and affect the ability of nations to get international support. Fraud against government programs can be used to fund organised crime groups and terrorism, potentially leading to further crime and terrorist attacks.

Financial impact

Based on international estimates, public bodies generally lose between 0.5% and 5% of their spending to fraud and related loss.The majority of fraud is hidden and undetected and can be difficult to categorise. Calculating the financial impact can assist agencies understand their potential losses and how to mitigate them.

Business impact

Business costs for dealing with fraud against government programs are significant and extensive and go well beyond the direct financial loss. They can include assessment, detection, investigation and response costs as well as potential restitution. In addition, further costs can include program review and audits and retrofitting or redesigning programs.

Introduction

Aim of the guide

This guide is intended to assist fraud specialists, government officials (including policy designers) and senior leaders to better understand the problem of fraud, and make a comprehensive argument on why something needs to be done about it.

- Senior leaders can use this guide to help inform their decision making
- Policy designers can use it to design services and counter measures
- Fraud specialists can use this guide to identify where to target counter measures, inform risk assessments, build fraud awareness and assist with narratives for investing in counter fraud initiatives

This guide outlines the main ways in which fraud can have an impact in the public sector, provides examples and case studies, and directs people to identify the impacts that relate to their program or public body.

Measuring the impact of fraud properly informs public bodies about their risk environment and aids their decision making. While measuring financial loss is key, other impacts can be just as (if not more) damaging to public services, the government that delivers them and, most importantly, the citizens that depend on them.

This guide is intended to articulate the main impacts of fraud. Not all impacts will be relevant to every public body or program. This guide assists public bodies to direct efforts to identify and measure impacts of fraud. It does not provide comprehensive methodology for measuring fraud or the cost benefits of counter fraud activity.

Background

This guide has been developed the Australian Government Attorney-General's Department on behalf of the IPSFF. The IPSFF recognises governments and public bodies face similar threats and risks of fraud despite their political, judicial, cultural and societal differences. IPSFF Member Countries identified the need for more comprehensive guidance for officials and executives to help them understand and articulate the scope and extent of the impact of fraud on their public bodies, the services they deliver and the citizens they serve.

IPSFF Fraud and Corruption Principles

The IPSFF has defined five key fraud and corruption principles in its Guide for Managing Fraud for Public Bodies (2019).

Human impact

Public bodies exist to improve the lives of the citizens they serve. Considering the human impact of fraud will help them approach fraud in a way that is most meaningful to those citizens.

While the direct financial loss is borne by public bodies, behind every story of fraud, there are real individuals, families and communities whose lives have been impacted or even destroyed. The damage to these individuals can be financial, physical or mental. Opportunistic individuals and serious organised crime groups target public bodies, including programs designed to assist vulnerable people, with little regard for the victims of that fraud. All too often the victims of fraud are those that already face the most challenges in their day to day lives.

Human impacts can often occur through the provision of sub-standard services or products, services or products being stolen or not being delivered, or identity theft. Impacts are not limited to individuals, but can also extend to their families and communities. Fraud can also impact physical safety.

Direct impacts on those who rely on government services

Fraud committed against public bodies, such as services being delivered by someone without qualifications, can directly impact those who rely on government services. For example:

- Money diverted by fraudsters out of payments and programs can mean that **victims miss out on essential services and supports that they rely upon.** As the money has not been used for its intended purpose it can also result in **lost opportunities** for the intended recipients.
- In addition to monetary losses, people affected by fraud against public bodies can **suffer serious psychological and emotional problems.** Victims of fraud have described experiencing a **wide range of emotional responses** including shame, embarrassment, distress, sadness and anger.
- People affected by fraud against public bodies suffer from **social problems** such as loss of reputation, feelings of vulnerability, isolation and exposure.
- Fraud can impact on a victim's **mental health,** resulting in anxiety, depression and suicide.
- The processes involved in dealing with fraud can result in **trauma** and **additional costs** from dealing with banks, insurance companies, utilities, law enforcement and advisors.

Identity theft

- Fraud against public bodies can result in individuals having their identity stolen. It can also be perpetrated through the use of a person's stolen identity. This can have long term impacts exposing the person to further fraud and potentially impacting their eligibility for services or benefits that they are reliant on.
- A failure to resolve financial and credit problems associated with fraud can have a detrimental long term effect on victim's financial health and ongoing credit ratings.

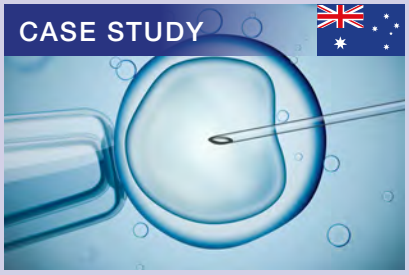
Family and community impacts

- Fraud can have far-reaching impacts beyond the individual, causing stress and disruption to **families and carers** as they try to help resolve the situation.
- Fraudulent behaviour can spread. When other people are seen to be committing fraud, individuals can **rationalise their behaviour** on the basis that if other people are committing fraud then it is okay for them to do it. They may also learn techniques to commit fraud themselves. Committing fraud can negatively impact individuals and their **family's lives** though increased stress and contact with the criminal justice system.
- Fraud against a public body may result in a **breakdown in social, governmental or industry trust** when people who have been impacted lose trust in everyday services and transactions. This can make these services and transactions more burdensome and lead to relationship breakdowns.
- Fraud can lead to other **businesses collapsing** which can leave their clients in a vulnerable position.

Physical safety

Fraud can put people's lives or health at risk by denying them essential services, or exposing them to unsafe activities, items or environments. Fraud can:

- Result in people having **unnecessary or unsafe** medical procedures
- Prevent people from receiving **essential treatment** or cause them to receive substandard treatment
- Expose people to **hazardous substances** or environments
- Lead to **vehicles or airplanes crashing** though faulty parts or maintenance
- Lead government agencies, including the military or police, to rely on faulty or unsafe **safety equipment,** such as bullet proof vests or bomb detectors, and
- Result in **faulty infrastructure,** which can lead to significant disruption and put people's lives at risk. For example, faulty runway lights at airports, bridges that collapse or cannot be used, and unsafe guardrails.



In Australia, a man falsely claiming to be a qualified in vitro fertilisation (IVF) specialist performed a range of treatments on 30 victims. The man, who never studied medicine, deliberately deceived his victims, defrauded them of A$370,000 and performing invasive procedures on their bodies. For some victims, they lost the opportunity to conceive a child through legitimate IVF providers. The court found the man acted without regard for the effects on his victims who were desperate to fall pregnant; breaching the trust they had in him, and encouraging false hope.

Between 2013 and 2017, a New Zealand government funded charitable trust set up to provide community services to people with intellectual disabilities was defrauded. The money intended to provide developmental opportunities to these people was stolen to fund the lifestyles of the trustees. As a consequence of this offending:

- The misappropriation of funds directly impacted individuals with mild to challenging intellectual disabilities. Over the course of the offending, they were not provided with the engagement that was intended to improve the quality of their lives.
- The persistent fraud also had an impact on the ability of the centre to employ staff (and on morale for existing employees), which in turn had serious implications for the quality of the service provided.
- The fraud impacted on the family and carers, who relied on the provision of care and support in order to be able to work.

The decreasing quality of service provided by the trust over time caused distress to the individuals accessing services, which in turn imposed additional emotional burdens on their caregivers.

In the United Kingdom, following the Grenfell Tower tragedy, police have investigated and charged contractors who installed defective fire alarms and emergency lighting in council tower blocks across London including Grenfell. The fraud put people's safety and lives at risk.

Following the tragedy, fraudsters were convicted of claiming £775,000 from a government fund that was created for victims. All of the individuals convicted either falsely claimed that they owned a flat that was destroyed, or that they had relatives who were killed as a result of the fire.

Frauds like this have diverted money from victims of the tragedy who have been left homeless and added to the distress of victims of the disaster.

In the United States, a health care facility owner led a decades-long, extensive health care fraud conspiracy involving a network of assisted living and skilled nursing facilities he owned. He bribed physicians to admit patients into his facilities and then cycled the patients through his facilities where they often failed to receive appropriate medical services or received medically unnecessary services billed to Medicare and Medicaid. Several witnesses testified to the poor conditions in the facilities and the inadequate care patients received.

Questions to ask:

- ? If your program was defrauded, consider the potential human impacts:
- ? Could fraud against your program result in mental health problems, psychological or emotional problems by individuals who should be benefiting from your program?
- ? If fraud diverted money out of your program, would the victims of fraud miss out on services, opportunities or payments they rely on?
- ? Could fraud against your program impact on the family or carers of individuals who should be benefiting from your program?
- ? Could fraud against your program result in financial stress or further fraud against individuals who should be benefiting from your program?
- ? Could fraud against your program put people's health or lives at risk?
- ? What more can your organisation do to take into account the human impact of fraud?
- ? How might these be addressed in any remediation plan?

Government outcomes impact

When fraud against a public body occurs, it diverts finite resources and compromises the government's ability to deliver services and achieve intended outcomes. This can happen in the following ways:

- **Services not delivered:** finite money and resources are diverted away from the intended target, or services are not delivered to the standard required.
- **Program objectives not met:** the vision, objectives, and goal of the policy or program are compromised.
- **Program/service shut down:** in some circumstances the entire program is shut down, which can negatively impact those relying on that service.
- **Customer/client experience:** the customer experience is compromised.
- **Opportunity cost:** fraud can result in lost opportunities to a program or service. Programs or services lose the opportunity to improve if shut down as a result of fraud, or if they are constrained by fraud financial losses and the business costs of responding to fraud.

CASE STUDY

Between 2016 and 2018 there was fraud committed against a Government funded Maori immersion school in New Zealand. This had the following impacts:

- The misappropriation of funds diverted government resources that were intended to improve educational outcomes for students.
- In addition to the direct financial losses sustained by the school, the inability to obtain sign off on their annual audits caused them to lose additional funding for equipment and resources for their students.
- The specific goal of revitalising Maori language, culture and knowledge through developing and expanding institutions (like Maori immersion schools) was not met.
- The broader government goal of improving educational outcomes for Maori students was undermined.

This manner of fraud diverts government money from being used for its intended purpose.

In the United Kingdom, a law firm created thousands of legal aid cases which never took place. An investigation found that out of the 24,658 mental health tribunal cases claimed for, a legal hearing had only been held for 1,485 of them.

The firm owner and his family lived a luxurious lifestyle on the government funds from these fraudulent cases, owning multiple properties globally.

The firm had a turnover of over £11 million annually and £8 million of this turnover came from the public purse.

Fraud like this diverts government money from being used for its intended purpose.

Questions to ask:

- If your program was defrauded, how would this impact on government outcomes?
- Could fraud result in services not being delivered? Which services? What would the impact be? What percentage of funding is actually reaching the intended target?
- How would fraud impact your program's objectives and outcomes?
- Could widespread fraud result in your program being shut down or restructured?
- If the money had not been diverted by fraud, what impact might it have had?
- What, if any, impact would there be on the delivery of services by other parts of the government or partners involved in your program?
- Are there any system flow-throughs to associated or ancillary programs or services?

Reputational impact

Public bodies that proactively manage their risks may be less vulnerable to reputational harm and can use their response to build confidence with other public bodies and industries, customers, the public and politicians.

However, reputational harm occurs when fraud could have been prevented or is mismanaged. Reputational impacts include:

- **Erosion of trust in government:** significant fraud against a public body may result in general erosion of trust in government. This can negatively impact how people conduct business at personal, industry and state levels. Other parties may not trust government with information, may feel a lack confidence in the government's ability to deliver programs or policies, or view government as a soft target for further exploitation. Erosion of trust in the integrity of the public sector has been shown to lead to a decrease in legal compliance.
- **Erosion of trust in industry:** fraud can result in not only loss to government, but can have further impacts on industry. Legitimate business in an industry where fraud has occurred against a government program can be tarnished by association.
- **Employee morale and performance:** knowledge of fraud occurring against or within the public sector can reduce employee morale and performance. This decreases productivity and compromises organisational culture. This can also lead to a culture of non-compliance where some level of fraud is seen as acceptable.
- **Damage to international and economic reputation:** fraud can impact the international and economic reputation of countries. Widespread fraud can be a contributing factor in assessments of whether a country is safe to conduct international trade and business, particularly where this is combined with corruption.

CASE STUDY

In the United States, a Department of Motor Vehicles employee and trucking school owner fraudulently issued commercial driving licenses to truckers who did not pass the required tests. People with fraudulent commercial licenses were driving passenger buses, tractor-trailers, and trucks hauling hazardous materials on interstates all over the country—putting the public at risk. The agency's failure to prevent unqualified drivers from receiving these licenses also affected citizens' trust in the agency, as well as public safety.

CASE STUDY

A PwC Global Economic Crime Survey found that reputation, brand and employee morale is the most damaging impact of fraud. The study highlighted that while it is difficult to quantify the cost of such collateral damage, it can ruin careers by association, deter employees, investors, suppliers and customers, and should be of real concern to organisations.

CASE STUDY

In Australia, the Therapeutic Goods Administration (TGA) identified that a company had been importing counterfeit condoms. The TGA proactively contacted customers who purchased the counterfeit condoms and organised a recall in addition to taking action against the supplier. The TGA's response received positive media coverage and boosted public confidence in the TGA.

CASE STUDY

In 2015, the Volkswagen Group was found to have intentionally distorted the emissions from their vehicles during emissions testing. This resulted in vehicles being sold with a lower emissions rating. On the first day of trading after this was uncovered, share prices fell by 20%.

CASE STUDY

In the United Kingdom, the Tower Hamlets County Council Mayor was removed from office after an election was overturned, due to evidence of vote-rigging and malpractice. An investigation found that ballots were double-cast or cast from false addresses.

Cases like this result in the public lacking confidence of those in trusted positions.

CASE STUDY

In Australia, vulnerabilities within the Home Insulation Scheme led to systematic fraud. The Australian National Audit Office found that in addition to causing serious inconvenience to households, and in some cases leading to death, the scheme caused reputational damage to the insulation industry and financial difficulties for many Australian manufacturers and installers. It has also harmed the reputation of the Australian government for effective service delivery.

Questions to ask:

- If your program was defrauded, what could be the reputational impacts?
- Could fraud result in a loss of reputation or erosion of trust in your program?
- Could fraud lead to an erosion of trust in your public body?
- Could fraud lead to an erosion of trust in Government as a whole?
- What would be the effect of an erosion of trust?
- Could there be reputational impacts to industry or your international reputation?
- What might be the impact on employee morale and productivity?

Government systems impact

The occurrence of fraud can result in costs and capacity drain in a wide range of government systems and services. Finite resources are diverted to deal with the fraud responses and outcomes. This reduces governments' abilities to deal with other issues. Examples of government system impacts include:

- **Investigations and compliance agencies:** public bodies with compliance and investigatory functions, including police and law enforcement, have finite resources.
- **Prosecution services, courts, tribunals and legal aid:** Court proceedings and legal representation are extremely expensive. Systemic fraud leading to a larger number of prosecutions may require government to provide additional funding for courts and legal aid organisations in recognition of the increased workload on the justice system. There can also be victim support costs.
- **Prison:** if prosecution of fraudsters leads to conviction, this results in prison costs.
- **Welfare system:** fraudsters who are caught may move to government welfare and other services for support and assistance. This results in additional cost on welfare and other government services.
- **Identification system:** identity fraud can lead to costs for authorities that regulate passports, permits and licences, eligibility to other programs, vetting systems and Fit and Proper Person checks.
- **Other public bodies:** where a fraudster has been accepted as a service provider, program recipient or employee in one public body, the documents generated can be used as proof of identity by another public body. Fraud occurring against one public body can enable fraud against another.

In the United Kingdom, Edwin McLaren and his wife were found guilty of property fraud totalling £1.6m.

The husband, who was said to be the "brains behind the scheme", was convicted of 29 charges and his wife of two.

Over a two-year police inquiry, 48 properties were investigated under a property fraud scheme where the owner's title deeds were transferred without their knowledge.

The trial at the High Court in Glasgow began in September 2015 and heard evidence for 320 days.

The trial was said to have cost around £7.5m, including more than £2.4m in legal aid paid for defence.

In the United States, a supplier of building products provided unsuitable and unsafe tools to a construction company that was contracted to build a tunnel. This resulted in a ceiling collapse which resulted in service disruption, as well as loss of life.

Questions to ask:

- If your program was defrauded, how would this impact on government services?
- What would be the impact and cost on the law enforcement and compliance system?
- What would be the impact on the prosecution service, the courts, tribunals and legal aid system?
- What would be the impact and cost on the prison system?
- What could be possible welfare system costs? Identification system costs? Impacts on other public bodies?
- What are the costs of retrofitting controls?

Industry impact

Fraud can have a flow-on impact on legitimate business and industry as a whole. For example:

- **Market distortion and competition:** fraudsters can gain a competitive advantage from engaging in fraudulent conduct. This can mean that legitimate competitors are priced out of the market and become bankrupt and close down. The fraudster can achieve a monopoly over the market.
- **Service impact:** services may not be fit for purpose, or may not be delivering what recipients want or need. When a fraudster is identified and their business shut down, but the fraudulent conduct led to market distortion and competitors closing down, recipients can be left with no service options.
- **System wide fraud:** fraudsters are agile and move between government programs as opportunities for fraud are closed down and others arise. Increasingly, fraudsters are operating across multiple programs or public bodies.
- **Exposes other industries and sectors:** fraud against public bodies can expose other sectors such the banking and insurance sectors.
- **Community services:** community services and charities can have extra burdens placed on them by fraud victims. For example victims may need to seek out financial, welfare, mental health and health care services. This may also reduce their ability to offer services to other often vulnerable people. Further, if a fraud has occurred within a community service, this may affect their ability to undertake and deliver their services. For example, people may be unwilling to engage with the service provider or they may no longer be in a position to perform their activities.
- **Increased regulation:** fraud within an industry can lead to additional regulation on an industry and legitimate businesses bearing the cost of additional checks and processes being brought in to combat systematic fraud.
- **Compliance resources impact:** industry wide fraud can use up capacity within an industry for compliance assessments and checks. This can lead to incomplete checks by unqualified or overburdened assessors, fraudulent assessors entering an industry and increases for costs for legitimate businesses. In addition, other burdens could occur such as costs for removing someone's professional qualification as a result of identifying fraud.
- **Integrity of industry is compromised:** where there is systemic fraud, this can compromise the integrity of the entire industry. Legitimate businesses can be tainted merely because they are part of an industry, and government and public can lose trust in the integrity of those businesses and their ability to deliver services. Widespread fraud can result in loss of trust in an industry as a whole.

CASE STUDY

In the United Kingdom, a group of education agents working at a number of government funded private colleges provided students with bogus qualifications in exchange for a share of their student loan.

For a fee students could fake their attendance at lectures, have their coursework completed by agents in Pakistan and receive a formal qualification which was the equivalent of a Higher Education degree.

Cases like this result in unqualified individuals being appointed in jobs they are not qualified or trained to do.

CASE STUDY

A fraudulent childcare learning centre in Penrith, Australia, was closed due to fraudulent activities. Due to outpricing, all other daycare centres in Western Sydney and other providers had to close down. When the centre was shut down there were no childcare providers left in the area, and community was left without adequate childcare.

CASE STUDY

In the United States, a Government Accountability Office (GAO) investigation found instances of producers adding undeclared or misidentified ingredients to dietary supplements. Another GAO investigation found that 20 of 47 items purchased from third-party sellers on popular consumer websites were counterfeit. Counterfeit and adulterated goods can threaten the health and safety of consumers and impact the public's trust in the reliability and safety of the industry.

Questions to ask:

- If your program was defrauded, how might this impact on industry?
- Could fraud result in market distortion or impact legitimate competition in business?
- What would be the impact on services provided?
- What would be the wider system impact?
- Would other industries and sectors be exposed or their integrity impacted?
- What would regulation would be needed to deal with systemic fraud if it occurred in an industry?

Environmental impact

In some cases, fraud can have an impact on the environment. Environmental damage can be immediate and direct, such as increasing levels of pollution, reducing biodiversity and disturbing ecological balance. These impacts can be medium to long term, or in some cases irreversible. Environmental impacts also include any clean-up and maintenance costs.

Fraud can also undermine efforts and the real or perceived effectiveness of green measures to improve the environment.

Studies have found that in countries where there are higher levels of fraud and corruption, environmental sustainability decreases.

CASE STUDY

Studies have estimated that approximately 59 premature deaths will be caused by the excess pollution produced between 2008 and 2015 by Volkswagen vehicles equipped with defective emissions devices.

CASE STUDY

Illegal, unregulated and unreported fishing is an example of a serious global problem with far reaching environmental impacts. According to a 2009 study, illegal fishing not only results in huge revenue loss, but can also threaten food security, particularly in less developed regions of the world.

CASE STUDY

In the United States, contractors substituted “clean dirt” for legitimate soil samples in order to fake the results of radiological remediation efforts at a former Navy shipyard. The falsification put the community and environment at risk, and the US Environmental Protection Agency (EPA) halted the transfer of additional land to real estate developers until the actual potential public exposure to radioactive material at and near the shipyard could be clarified.

CASE STUDY

A United States mineral company engaged in fraudulent activity in an attempt to bypass environmental remediation costs and responsibilities for cleanups at toxic sites around the country. This company fraudulently transferred its valuable oil and gas assets to a "new" company, leaving the original company with only legacy environment liabilities. The original company later declared bankruptcy, as it had insufficient assets to pay the billions of dollars of liabilities that it owed to environmental regulators, the Navajo Nation, and others.

This posed a significant threat to the environment and local communities.

CASE STUDY

Alleged corruption occurred within a New Zealand local government body in relation to the awarding of a contract for an important local infrastructure project. The tender process under scrutiny resulted in the contract being (initially) awarded to an unqualified organisation and risked serious immediate and long-term health risks to the community who were relying on this project being delivered safely.

Questions to ask:

- ? If your program was defrauded, what environmental impacts may result?
- ? Would there be any immediate environmental damage?
- ? Would there be any medium to long term environmental impact?
- ? Would fraud undermine green initiatives?
- ? Would there be any clean-up costs or environmental maintenance costs?

Security impact

Fraud can have an impact on security, including national security and the security of individuals and organisations. Security impacts can include:

National defence: where fraud compromises security, it can impact a nation's ability to effectively defend its sovereignty and its citizens. This can put the lives of its service men and women, as well as citizens, at risk.

National security: fraud can compromise national security and community safety when perpetrated by organised crime groups and terrorist groups. For example:

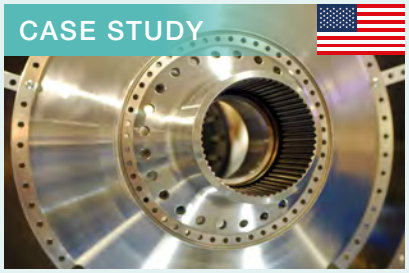
- *fraud being undertaken by actors for the purposes of funding terrorist activities;*
- *organised crime groups using proceeds of fraud to perpetrate other criminal activities; and*
- *compromise border security resulting in biosecurity risks and enabling trafficking of illegal goods.*

- **International standing:** fraud can result in a falling in international standing, for example where operations fail or are compromised due to faults in defences, weapons, technology or machinery
- **Organisation security:** fraud can compromise the security within private sector or non-public bodies. This can have a flow on to compromise in national security, for example where fraud involves identity theft, or where there are links with government services or systems. Further, where trusted insiders are exploited by serious and organised crime groups or innocent persons are coerced by these groups, this can put organisational security and personal security at risk.
- **Information security:** where information leaks out from public bodies due to fraud, this leads to reduced trust, and reluctance by the public to provide government with secure information.
- **Other nations:** fraud can result in threats to other nations though international entities using material obtained fraudulently in one country to commit fraud in another (for example, obtaining false passports) or transferring fraud methodologies to target programs in other countries.

CASE STUDY

In the early 2000s, fake bomb detectors were sold to twenty countries in Asia and the Middle East. These faulty detectors were subsequently used by operational personnel to guard airports, protect hotels, and in security sweeps, with significant human and security risks.

The United States GAO found passports that had been issued to applicants who used identifying information of deceased or incarcerated individuals, had active felony warrants or used an incorrect Social Security Number. Fraudulent passports can be used to facilitate further crime such as drug trafficking or international terrorism.



The United States Department of Defense was defrauded of more than US$11.2 million dollars by an international conspiracy supplying nonconforming and defective parts for military aircraft, vehicles, weapons and systems. This put the military at significant risk of harm.

Throughout the 1990s, members of al-Qaeda learned to exploit weaknesses in the US immigration, passport, visa and entry systems. They successfully instituted a travel facilitation operation in Afghanistan through the use of travel agents, document forgers, and corrupt government officials. The 9/11 hijackers employed a variety of methods to conceal their identities, including the use of 364 aliases, fraudulent entry-exit stamps, and altered passports. Through these fraudulent methods, the 9/11 terrorists obtained legitimate passports and tourist visas, entered the United States, and perpetrated the largest terrorist attack in US history.

Questions to ask:

- ? If your program was defrauded, what impacts might there be on security?
- ? Would there be an impact on national defence or national standing?
- ? Would there be an impact on the security of information?
- ? Would there be an impact on the security of organisations that engage with government?

Financial impact

Why measure the financial cost of fraud?

Measuring the financial cost of fraud is challenging. Fraud is a hidden crime and by its nature difficult to detect. In many cases, public bodies might not be able to detect all fraud occurring against them. In addition, public bodies might not be able to identify whether a matter was fraud until many years after it occurred.

However, measuring the financial cost of fraud is crucial in order for agencies to conduct their business effectively. Calculating the financial loss that results from fraud helps to demonstrate the significance of the fraud problem. Measuring the financial loss resulting from fraud provides a metric from which the public body can make decisions on how much it should invest.

For instance, if a public body that spends $1bn knows that it loses an estimated 2% of its budget to fraud and related losses ($20m), it is more likely to proactively invest in counter fraud resources and controls to supress and reduce this number than a public body that does not know whether it loses any of its budget to fraud.

While estimates vary, there is no doubt the financial cost of fraud is significant. For instance, in the United Kingdom, public bodies are estimated to lose between 0.5% and 5% of their spending to fraud and related loss. This equates to £31bn-£48bn lost every year. In Australia, the estimated financial loss to fraud is A$5-25 billion per year.

In the absence of a financial measurement, spending on counter fraud can be deprioritised in favour of spending to mitigate more tangible risks, threats and opportunities.

Methodologies for calculating the financial impact of fraud

The following are some of the categories of data to consider when assessing the financial impact of fraud loss.

Indicated Fraud

- There are range of metrics that can be used to indicate potential instances of fraud within a business. These metrics can include referrals, intelligence, investigations started and, potentially, identified anomalies in the system.

Detected Fraud

- A number of different metrics are used when considering detected fraud. These are considered in more depth in **Annex C**, alongside their strengths and weaknesses.
- Detected fraud is a measure of the financial loss that a public body is aware of. It is not a measure of total loss in the organisation, but rather the amount that has been uncovered and accepted (at some level) by the organisation.
- Often, the detected fraud level in an organisation can be supressed by reluctance, in that organisation, to accept fraud without a very high burden of proof.

Estimated Fraud Levels

Only a proportion of fraud against an organisation is ever detected. Organisations can estimate the level of fraud within some of their payments and systems through:

- Carrying out fraud loss measurement exercises within discreet areas of their organisations (either random and risk targeted).
- Finding a measurement exercise (or exercises) carried out in closely comparable areas of spend to those in your context. These exercises could then be used as a proxy in the absence of a measurement exercise.
- Researching fraud measurement exercises more generally, and reaching a considered view on the likely range of the potential proportion of fraud that could be found. This range could then be applied to the organisation.

Fraud measurement exercises take a statistically valid sample from a payment or income area and test the sample for the presence of fraud by considering specific risks and whether they have come to pass. Where fraud is found this is then extrapolated across the population.

It should be noted that many fraud measurement exercises consider both fraud and error. The difference between fraud and error is the intent of the people involved. Establishing intent can be overly expensive for some organisations (it requires further investigation), especially if they are satisfied by an understanding of the overall fraud and error loss (rather than the breakdown of what was intentional and what was not).

The different approaches outlined above will result in different qualities of evidence (in descending order). The best evidence that is available should be used and it should be remembered that an indication, based on the best evidence available, is often better than an absence of evidence – especially when it is remembered that fraud is a hidden crime. However, those using evidence on fraud should be transparent on both the limitations of their evidence and the widely accepted inherent difficulty in defining financial loss from fraud.

The UK's Fraud Measurement and Assurance programme, provides a comprehensive methodology for estimating fraud levels in an area where there is a high risk of fraud.

Unknown Fraud

Measurement exercises take a sample of payments or situations where fraud may have occurred and consider whether specific fraud risks have occurred in that sample. In addition, if the sample is risk targeted, it might not reflect total fraud across the organisation. The nature of fraud is so diverse and quickly evolving that it is not possible to consider all fraud risks when undertaking a measurement exercise.

As such, there is always likely to be an element of unseen, unmeasurable fraud loss within an organisation of a significant size. This cannot be measured, but those considering the financial loss resulting from fraud should be aware.

Recovered Fraud Loss

Some detected fraud is subsequently recovered by the organisation. In some circumstances organisations offset this recovered loss against their detected loss to give a more accurate view of the financial impact of the detected loss. However, when doing this any business-related costs in the investigation and recovery of that fraud should be taken into account.

In 2017 a department in the United Kingdom undertook a fraud measurement exercise to quantify patient prescription fraud.

Some groups of people are exempt from paying for prescriptions based on their income and age. The exercise wanted to identify those who were fraudulently claiming for free prescriptions.

The measurement exercise identified 2.8% of fraud and error combined, equating to £167.8 million lost to fraud.

A UK government department undertook a fraud measurement exercise on one of their loans offered to university students in 2015/16.

They looked at students declaring their marital status, which is used to assess the value of the loan that a student is entitled to receive.

The exercise found that a number of students were mis-declaring their marital status and that of their spouse.

This exercise found that 11.7% of the tested expenditure was fraud and error.

A UK government department undertook a fraud measurement exercise on its use of bus operator grants. The grant had a number of exemptions including school buses and bus tours (where the bus company makes its own financial gain).

The fraud measurement exercise identified a number of cases where the grant had been misused for school bus routes. They also found that some recipients had inflated mileage claims.

The exercise found that 9.2% of the tested expenditure was fraud and error.

Questions to ask:

- ? Do you have any reliable data on the financial cost of fraud to your organisation?
- ? Do you know the level of detected fraud in your organisation? Does the organisation understand the limitations of these numbers?
- ? Do you have an estimate of the total level of fraud in your organisation (noting that the detected level and total level are not the same)?
- ? Are there any comparators you could use from other public bodies, other administrations or other sectors to provide a view of the potential level of fraud?
- ? Is the nature of measuring the financial loss as a result of fraud understood by those who will be reviewing the numbers or taking decisions based on them?

Business impact

Business cost of responding to fraud

The cost of responding to fraud once it has occurred cannot be discounted. These costs are significant and extensive, but often overlooked. However, these costs can be identified. Measuring these costs can help demonstrate a more complete picture of the actual financial cost to a public body. Considering business costs can also highlight the importance of investing in preventative measures, which may be comparatively lower. These costs include:

Assessment costs

As allegations or referrals of fraud are received, resources (staff, time and systems) are required to assess whether to investigate.

Detection costs

If public bodies are detecting fraud, this will take resources. Detection costs may be spread across the public body and across public bodies. Detection costs could include building in detection to program design, compliance checks, organisation-wide fraud detection, tip-off arrangements, data analytics programs, technology tools, training and data sharing between public bodies.

Investigation costs

Fraud investigations can be resource intensive. Understanding these costs can help a business prioritise in prevention rather than reactive investigation.

Investigation costs include the costs of briefing and resourcing investigation staff, both internal and external. Investigation costs will vary depending on the size and complexity of the fraud and may not necessarily correspond with a public bodies' fraud risk (for example a public body with a large fraud risk may have simple matters to investigate while a public body with a small fraud risk could be victim to a complex fraud that is very resource intensive to investigate). Investigation costs can continue over many years where the investigation staff are required to give evidence in court proceedings or review findings from a matter to highlight vulnerabilities in a program.

Response costs

Once fraud is identified and a decision is made to take action, this requires additional resourcing.

A decision may be made to prosecute the fraudster. Court and tribunal actions can be resource intensive. Resources are required to support the court process with prosecutorial briefing and evidence gathering, and legal representation (both for the public body, persons affected by the fraud and potentially the offender) and advice is very costly.

Administrative action may be taken in response to fraud such as cancelling a service or cancelling a person's participation in a program. Administrative action consumes organisation resources in terms of time and briefing. Administrative actions are subject to appeal in court, which has costs associated. Chasing up recovery of funds following administrative action can be expensive as well.

Restitution for third party victims

Members of the public can be impacted through fraud. Public bodies may need to allocate resources to restoring services to them and potentially compensating them for losses due to fraud. Cost can include setting up new accounts and restoring lost identities.

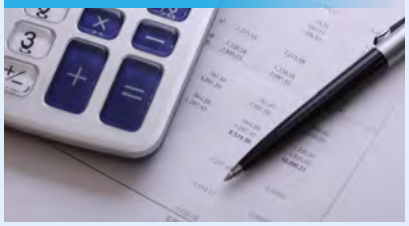
Program review and audits

Once fraud is identified, this may result in a program review or audit. Program reviews can often require external consultants. In widespread and systemic cases of fraud, this can result in a broader review such as a Royal Commission. Additionally, the program could be selected for a performance audit. The Australian National Audit Office reported in its 2018–19 Annual Report that the average cost of a performance audit report in 2018–19 was $419,000.

Retrofitting or redesigning programs

When fraud shows vulnerability in program and policy design, programs can be redesigned or retrofitted to deal with these vulnerabilities. This has a cost in terms of time and resources from a variety of areas (for instance, policy, process design, operations, project management and digital).

CASE STUDY



If an organisation receives 100 allegations of fraud each year and it takes 5 hours to review each allegation, if an hour of employee time is $40 (building in on costs), it will cost the organisation $20,000 to do the reviews.

If the same organisation investigates 20 of these allegations for fraud a year, and it takes 800 hours to investigate these allegations, with an hourly cost of $60 (building in on costs) it will cost the organisation $960,000 to investigate the fraud cases. This is not including the additional costs of recovery/sanctioning.

In total, to investigate fraud it is costing the organisation $980,000 a year.

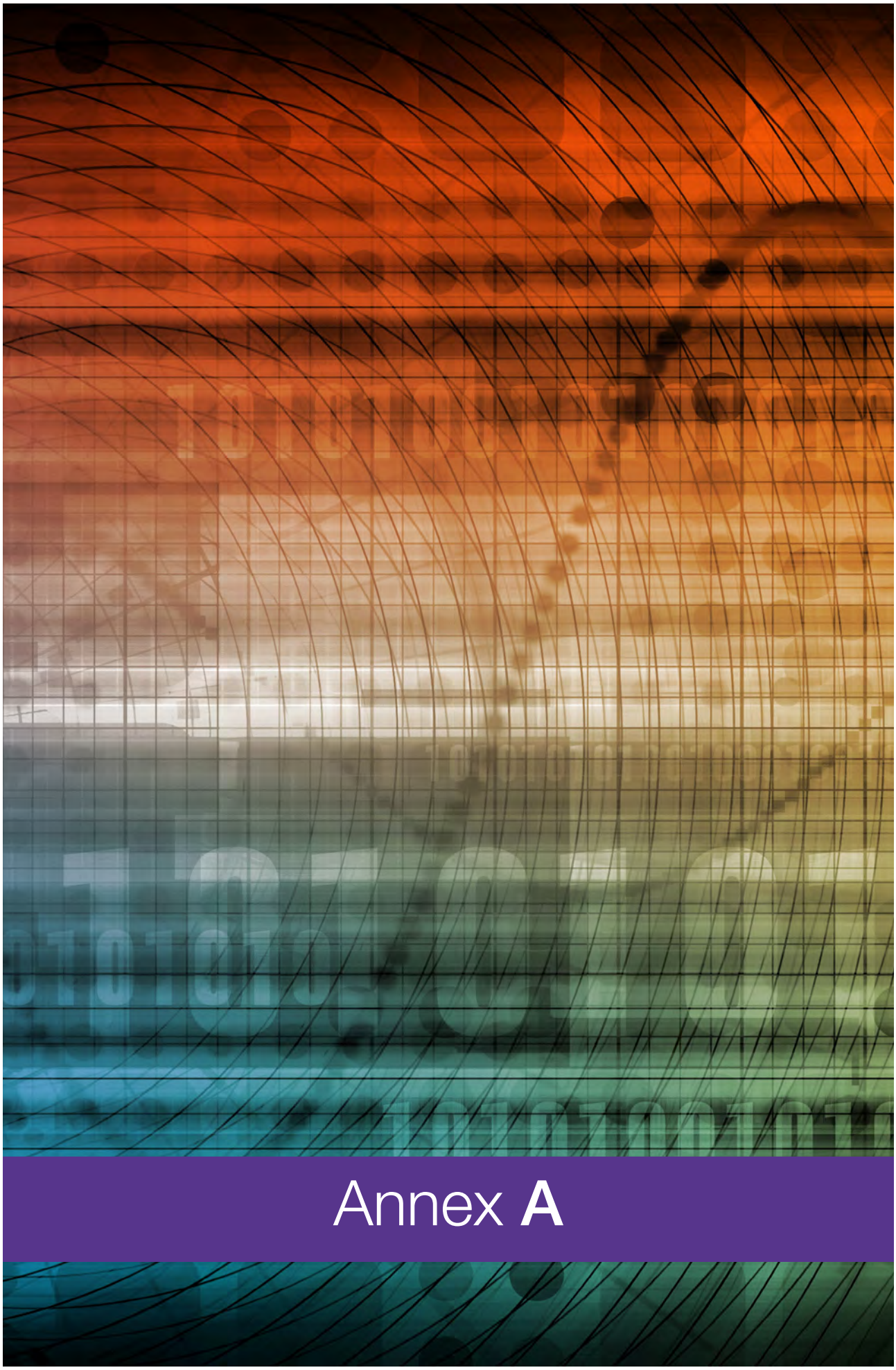
CASE STUDY

Australia's Home Insulation Program subsidised insulation as part of an economic stimulus package. The scheme was plagued with cost overruns, fraud, home fires, injuries, as well as the deaths of four installation workers.

These outcomes had significant business costs, requiring the establishment of a royal commission (approx. A$20 million), an independent review, audit costs, compensation costs to insulation companies (approx. A$500,000) and remediation for impacted individuals.

Questions to ask:

- Do you understand the wider business costs required to respond to fraud?
- Do you understand how many allegations of fraud are made per year and how many are investigated?
- What is the business cost of assessing whether to investigate these allegations?
- What is the cost of investigating one single allegation of fraud against your program?
- Do you understand the costs (premises, equipment, training, tax, pensions, expenses etc.) of your counter fraud resources?
- What is the cost of fraud investigations for your program per year?
- How much is being spent by your program on detecting fraud in your program? What other parts of your organisation or other public bodies are investing in detecting fraud in your program?
- Can you calculate the cost of investigating fraud in your business?
  - *Do you know the average cost of an allegation review and an investigation?*
  - *Can you compare the cost of increasing your organisation's internal investigators to the cost of sourcing consultants to respond to fraud investigations?*
- Might identified fraud result in an audit? If so, how much would this cost?
- Can you estimate how much a potential review of a program with fraud problems could cost your organisation?
- Might identified fraud result in retrofitting or redesigning your program? How much would this cost in terms of time and resources?



Annex **A**

Annex A - Case study demonstrating multiple impacts – NDIS

Each case study contained in this guide was used to demonstrate a particular impact. However, each of these examples of fraud had multiple impacts in different spheres. This case study demonstrates how fraud can have multiple and wide-ranging impacts.

Since its introduction in 2013, fraudsters have targeted Australia's National Disability Insurance Scheme (NDIS, or the Scheme) delivered by the National Disability Insurance Agency (NDIA). The NDIS is one of Australia's most important social reforms and aims to provide around 460,000 Australians aged under 65, who have permanent and significant disability, with funding for supports and services. With the NDIS, people with disability are at the centre of the system - participants choose their providers, rather than providers being contracted by government agencies.

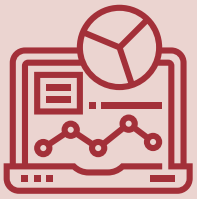
The NDIS was established to provide major benefits for people with disability, their families and the broader community. However, when the program was defrauded, it was vulnerable people who were in fact most heavily impacted.

Human and society impact

Fraud against the Scheme has far-reaching and devastating impacts on NDIS participants, resulting in the inability to purchase essential supports (such as incontinence aids), the disruption of routine (including missing appointments or work commitments, therapy and social outings) and a ricochet effect on carers and family. By taking money directly out of NDIS participant plans, it reduced people's ability to obtain crucial assistance and services to help them lead their lives and access ongoing support.

Reputational impact

Fraud occurring against the NDIS resulted in the Federal Government establishing the NDIS Fraud Taskforce in July 2018; a multi-agency partnership between the Australian Federal Police (AFP), the NDIA and the Department of Human Services (DHS). The Taskforce deals with the high risk and serious criminal activity targeting the NDIS.



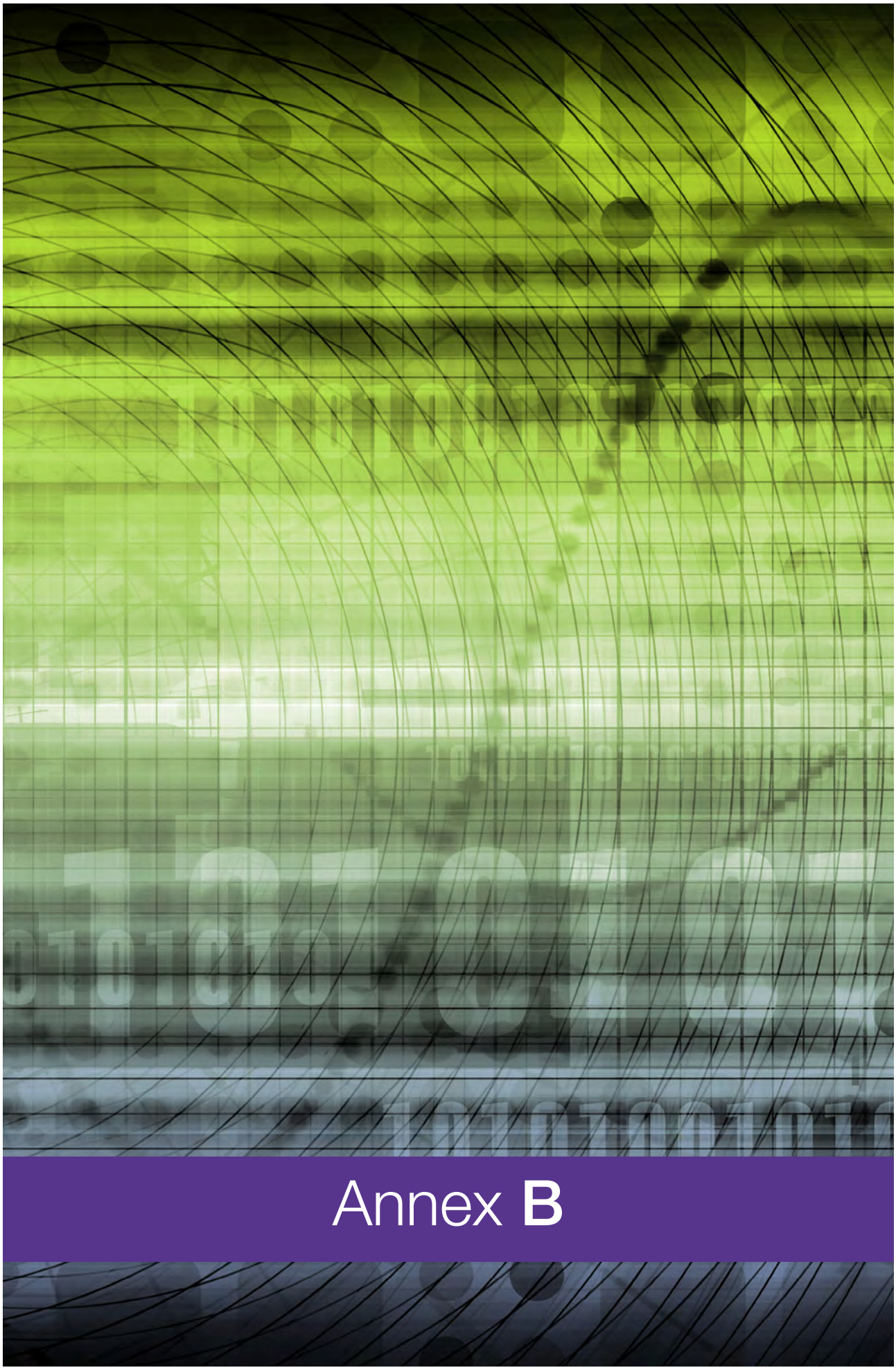
Government and business impact

NDIS is a generational change in how services are delivered to people with a disability. The NDIS was targeted by organised criminal syndicates using the provider model to defraud the scheme of millions of dollars by making false claims, over-inflating the costs of services and falsely drawing from NDIS participant plans. This led to a loss of confidence in the government's ability to deliver the Scheme.

Financial impact

The NDIA is set to receive A$20.2 billion in 2019–20 to deliver the Scheme. There are currently a number of investigations underway with an estimated value of approximately A$9.3 million into alleged fraud against the scheme.

The NDIA has developed a targeted fraud approach, focussed on the protection of participants and the sustainability of the scheme. By establishing a suite of proactive and reactive fraud capabilities, including the active Fraud Taskforce, they are able to better identify and deal with fraud, and protect and support participants as intended.



Annex **B**

Annex B - Considerations when measuring financial cost

When calculating financial cost, consider the following:

Fraud numbers are often misunderstood or incorrectly presented

There are many different aspects to fraud numbers and simple concepts, such as detected fraud, can be interpreted in a number of ways (for instance, whether these are cases which have been bought to trial or cases under investigation). Many public bodies are dependent on their figures on detected fraud or prosecuted fraud as a measurement of their fraud loss. Evidence from organisations which have both metrics of detected fraud and estimates of their fraud loss through statistically valid measurement exercises indicate that a detected metric does not reflect the actual loss the business is likely to be suffering. However, the understanding of this at an Executive/Board level is not consistent.

Estimating fraud loss is complex and can be resource intensive

Fraud measurement is not a simple exercise. To be effective, it takes resources to both thoroughly understand the risks in that area and to test for the occurrence of fraud. This kind of testing is beyond what you would expect to see in a standard audit. The resource commitment can also be increased if the business is looking to produce a statistically valid estimate. However, some evidence is better than no evidence. It is often better for a public body to do some fraud measurement with limited statistical validity rather than not do any measurement activity.

The nature of the public sector makes fraud measurement especially complex. Public sector organisations have many diverse spending and income streams and the fraud risks and threats are often different in the different areas. This means that different measurement exercises would be needed in each area to build a comprehensive view. The number of different payment streams can make this prohibitive. It is possible to use comparators from similar payment streams, but the limitations of this approach should be recognised.

There are a variety of different methodologies

There is no single, internationally recognised methodology for measuring fraud loss. The methods used in different contexts differ, as can the classification of the results. For instance, in the United States, the measurement of improper payments takes into account fraud, error and where procedures have not been followed, while in the UK the focus is on fraud and error. In some areas fraud measurement exercises state that they focus on fraud loss alone, while others look at both fraud and error loss.

This means that it is important for an organisation to understand the methodology that it is using to measure fraud loss, its strengths and, most importantly, its limitations. All fraud measurement methodologies have limitations.

The relationship between fraud and error should be understood

The difference between fraud and error is intent. To identify intent, an investigation has to be undertaken, which can be a significant investment in resource. There are a number of reasons that investigations may not be undertaken, for example awareness of the potential for fraud, organisational willingness,

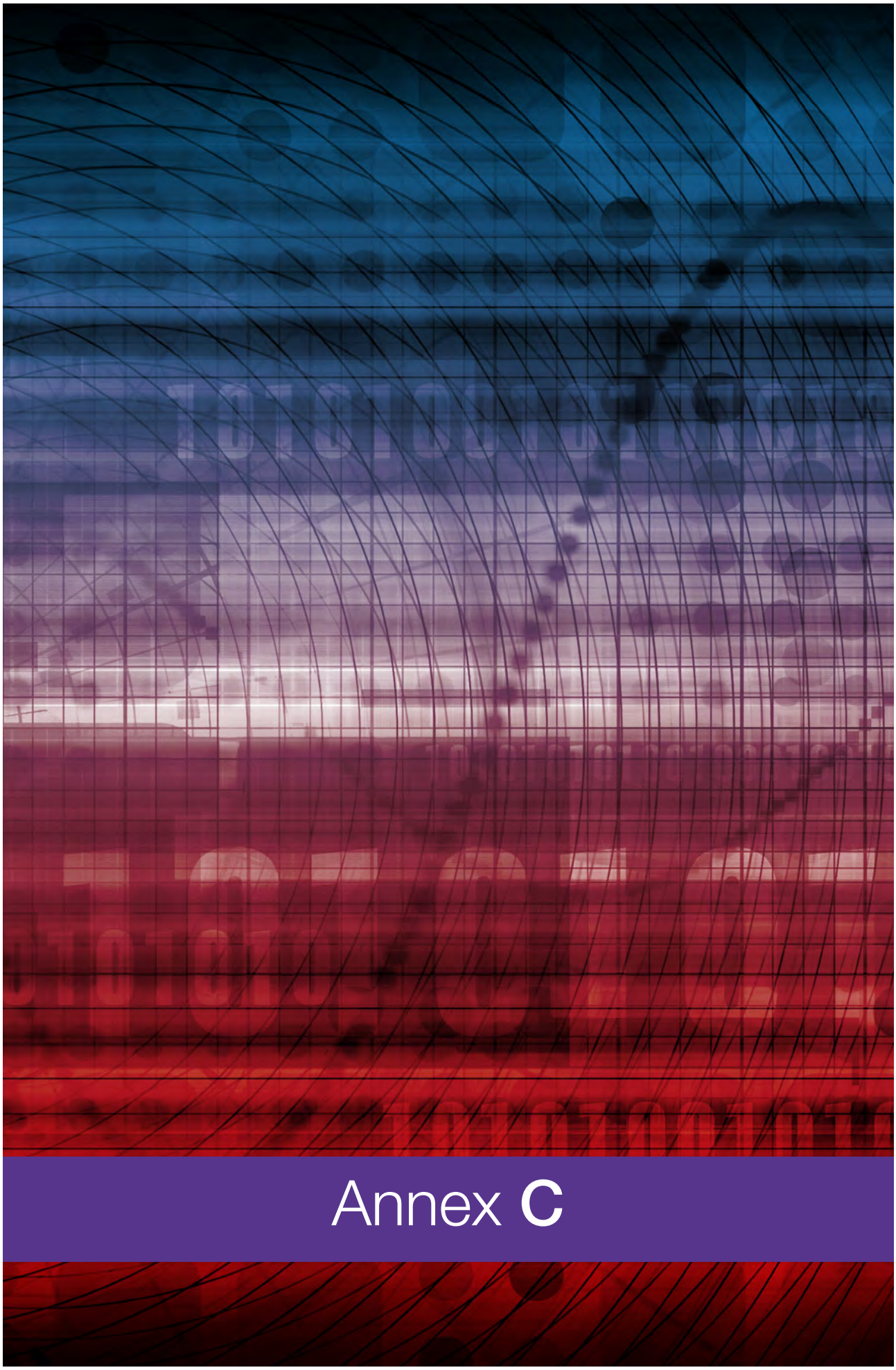
and available resources. Organisations can often be unwilling to consider whether a payment is fraud as opposed to error. It should be remembered that where a payment has been made or a service given, even if it was a genuine error, it demonstrates that fraud could take place – as an individual with intent could take the same route. Often when considering total potential fraud exposure, it is practical to take some of what may be error loss into account. This is because it may not be worth the investment to establish if individual cases were fraudulent and the presence of the irregularity shows a control vulnerability that could be taken advantage of by fraudsters.

Financial estimates are usually an underestimate

When financial estimates (fraud measurement exercises) are undertaken they check a payment area against specific fraud risks. Fraud risks within a system are numerous and usually it is not possible to test all of these risks in a measurement exercise. In addition, some fraudsters may hide their activity so it is difficult to identify them through a random sampling approach and even if they are detected, the fraud's total cost may not be identified. As such public bodies should be aware that fraud measurements and estimates are usually underestimates.

Focusing on financial impacts can lead to the broader impacts of fraud being overlooked or underappreciated.

An over emphasis on the financial impacts of fraud can led to public bodies overlooking the other, non-financial impacts. For instance, a public body may be tolerant of public money being lost to fraud. However, they may not be so tolerant of the damage to the organisation's reputation that could result from the fraud and could lead to a breakdown in trust between the public body and the government or the public. It is important for those working in fraud to make sure senior leaders and Ministers are aware of the range of impacts that may result from a fraud.



Annex **C**

Annex C - Strengths and weaknesses of individual fraud measures

The following appendix gives an indication of the strengths and weaknesses of the different types of financial fraud measures that are used. Understanding these helps those working on fraud or leading organisations to understand the numbers they are being presented with or using.

Indicated Fraud

Anomalies in data

When undertaking proactive fraud detection work, analysing or sharing data, anomalies in this data may be identified. It may also be identified in business as usual activity. Anomalies in data do not themselves indicate fraud, but rather a potential that something is not right. Further work is usually required to confirm if there is anything worth considering from those anomalies. Depending on the anomaly and how it has been found, some may consider these fraud referrals, where as some others may be considered as a stage before referrals. The false positive rate (number of instances where no fraud or irregularity is found) on data anomalies can often be high, especially when new data shares or analytical techniques are being used. Nevertheless, anomaly detection can help you target your resources for fraud detection.

Referrals

Referrals represents the number of referrals for potentially fraudulent activity an organisation, or that an organisation's fraud team, have received. This does not represent the level of fraud loss in the system because:

- Only a proportion of these referrals will actually represent fraud;
- Only a small proportion of fraud is likely to be referred through an organisations referral mechanisms.

Different organisations may define referrals in different ways. For instance, some organisations may include all referrals made to a whistle-blowing line, while some organisations may do an initial sift to exclude any that, for instance, are known not to be possible or in scope of their organisation.

Increasingly, organisations are using data and analytics products to detect and prevent fraud. Where this is the case, analytics products produce 'indicators' of fraud or irregularity. These may be seen as fraud referrals, but it should be remembered that the vast majority of these 'indicators' need further analysis to establish whether they are flagging a risk of fraud or some other type of discrepancy.

Referrals may contain information on the financial value of fraud. However, it should be noted that at this stage this is likely to be unreliable, as the allegations in referrals have not been substantiated. As such, the more reliable value is the volume of referrals.

Intelligence

Where referrals are seen to have elements that require further consideration, they may then be identified as intelligence. What referrals are, or are not, considered intelligence could be assessed in a number of ways, and will often be driven by organisational practices. As such, any metrics around intelligence will be driven by the intelligence assessment practices of the organisation that reports them.

Intelligence could also be considered from different lenses. For instance, one referral may include several different potential instances of fraud. When this is the case, the organisation may break down the individual instances separately. As such, reported figures on intelligence may include a number of frauds within each intelligence item or may be broken down by all the individual instances.

Those considering metrics around intelligence should also be mindful of the difference between the intake of intelligence (when an item is initially recognised as intelligence), and the worked items of intelligence (those that have been reviewed and developed).

When considering figures on intelligence items, it should be acknowledged that these figures do not represent detected fraud, as some items of intelligence with be demonstrated not to be fraud, and some items will lead to the uncovering of more fraud.

Intelligence may contain information on the potential financial value of fraud. However, whilst this may be more reliable than any figures at referrals stage, any financial figures are likely to still be unreliable, as the intelligence may not have been substantiated.

Volume metrics will be more reliable, but the composition of these figures should be taken into account when using them.

Administrative fines and sanctions

When undertaking compliance work and irregularities are discovered, an organisation may make a decision not to investigate whether there was intention in the irregularities, but rather to apply any sanctions and administrative fines that are available to it. Administrative fines and sanctions may be a helpful metric when trying to consider the broader picture of fraud and error (irregularity) loss within a business.

Investigations started

An investigations started measurement measures levels of potential fraud from the number of referrals where an investigation has been formally commenced. This can be both a volume (number of investigations) and value (potential value of fraud within the investigations) metrics. This metric has the advantage of being a more stable and objective metric.

However, its limitations should also be recognised, specifically:

- Investigations started is as much an indication of the capacity of the organisations to investigate as it is a metric of the level of fraud allegations which could be taken to investigation. When an organisation takes the decision to investigate, it both considers whether the allegation has merit and its capacity to take on an investigation;
- Investigations can vary from one, simple act of fraud up to a complex fraud with multiple acts from multiple and overlapping individuals. As such, one recorded investigation may include several instances of fraud within it;
- Some potential frauds that are investigated either are not demonstrated to be fraud, or are demonstrated to not be fraud. As such, the metric will contain some investigations where fraud is not ultimately detected.

Investigations Completed

An investigations completed metric identifies the cases where investigations have been concluded. This can be both a volume (number of investigations) and value (financial value of detected fraud) metrics. The financial value of these cases is much more reliable than the other metrics, as the investigation has been completed, which means there are fewer uncertainties. However, it should be noted that some investigative approaches will focus in on a part of the overall allegations – so the financial level detected still may not encompass the totality of the potential fraudulent activity from the allegation it is related to.

It also has further limitations:

- Investigations may be closed for a number of reasons, including capacity, likelihood of success and whether allegations are found to be supported
- Investigations can vary from one, simple act of fraud up to a complex fraud with multiple acts from multiple and overlapping individuals. As such, one recorded investigation may include several instances of fraud within it;
- There can be a significant time delay to the completion of an investigation;
- Different organisations may classify the end of their investigations at different points. For instance, some may classify it as when the case is handed to prosecutors, some when it reaches court.

Detected Fraud

Detected fraud to the civil balance of probabilities

A further way to consider reported levels of fraud is 'fraud based on the civil balance of probabilities'. This is the method used in the UK for fraud data collected from public bodies and then published by government.

The advantage of this is it reduces the false positive rate that may be reported through referrals and intelligence, as organisations only report once they have reached a view that the referral is likely to be fraud. The civil balance considers whether the allegation is 'more likely than not' to be fraud. This contrasts with the criminal balance, which is 'beyond reasonable doubt'.

Again, consideration should be given as to whether a single reported fraud might include multiple allegations of fraud.

The weakness to this as a metric is that the civil balance is a subjective test. As such, different organisations may evaluate what is more likely that not to be fraud according to different internal rules and guidance (or even with a lack of guidance). For instance, an organisation that has limited understanding of fraud and is very risk adverse in labelling any received referrals as fraud will have a proportionally lower level of detected fraud to the civil balance than an organisation that is open to fraud and actively seeking it.

Settlements and Plea Bargains

Courts can agree on a settlement, or a plea bargain with those who have allegations of fraud against them. Depending on the circumstances these cases, and the financial recompense associated with them, can be considered as detected fraud (against the civil balance) for an organisation looking to measure the extent of fraud. However, it should be taken into consideration that the settlement or plea bargain may not cover the full extent of potential fraud. It should also be considered whether any settlement includes any aspects beyond what may be allegations of fraud. Further, some settlements will involve a forfeiture but no admission of guilt.

Proven fraud and Criminal Justice Outcomes

This metric considers allegations where it has reached a final criminal justice decision on whether fraud took place, such as a finding in a court of an admission of guilt. It can be measured both on volumes and financial value.

This metric represents a fraction of potential fraud in a system, as it is the allegations that are both detected and taken through to criminal justice conclusion. Only a proportion of fraud is detected, only a proportion of this is investigated and only a proportion of investigated fraud will reach a criminal justice outcome or proven fraud.

Proven fraud and Criminal Justice Outcomes cannot be used as a reliable measure of the financial impact of fraud on an organisation as it disregards the undetected and not investigated instances of potential fraud.

Recovered Fraud Loss

Following compliance and investigative activity, fraud that is detected may well go into a debt recovery process. Some of the detected fraud will be recovered through that process. Ideally this should be recorded and reported separately to the other metrics.

In some circumstances, organisations take the level of recovered fraud loss into account when considering fraud loss. However, it should be recognised that:

- The recovery of the debt involves a cost. Recovering in full a detected fraud loss, does not necessarily mean that the fraud had a net zero cost to the business;
- There can be a significant time lag for the collection of debt;

The netting of recovered detected fraud from detected fraud levels can be confusing and if this is done it should be made clear that this has been done, including the methodology.

In some instances, following a fraud, financial sanctions (such as fines or contract penalties) may be taken. These should be considered separately and not netted off the detected fraud loss.

Prevented Fraud

An organisations activity to find and fight fraud will prevent some fraud losses; either through stopping would be fraudsters before they are successful (for example, through effective application controls or billing reviews) or through stopping ongoing fraudulent behaviour before it is complete (for example, through audit or review of ongoing contracts or services). This broadly breaks down into these two categories:

- Fraud stopped before loss
- Loss reduced through stopping fraudulent activity part way through.

The diversity of fraudulent activity can make it difficult to accurately measure the level of fraud prevention. For example, if a fraudster's activity is disrupted, it can be difficult to establish how much longer they would have continued the activity.

There are a number of different ways to measure the level of prevented fraud in an organisation. However, it is sensible to exercise caution over the methods used, and to ensure they are independently challenged to ensure the robustness of the figures. In the UK, for example, all prevention methodologies are reviewed by a cross government 'Prevention Panel'.

Deterred Fraud

An organisations activity to find and fight fraud, and the promotion of it, can deter would be fraudsters from committing fraud against that organisation. This is notoriously difficult to identify and measure, as much deterrence happens before an individual physically interacts with the organisations systems.

Estimated Fraud

Fraud is a hidden crime and businesses cannot assume that all fraud has been detected. It is extremely unlikely that the detected fraud within an organisation will represent the total financial impact of fraud on that organisation, or the total loss from fraud they have experienced.

Increasingly, public bodies are undertaking fraud loss measurement exercises to establish the undetected level of loss within a part of their organisation.

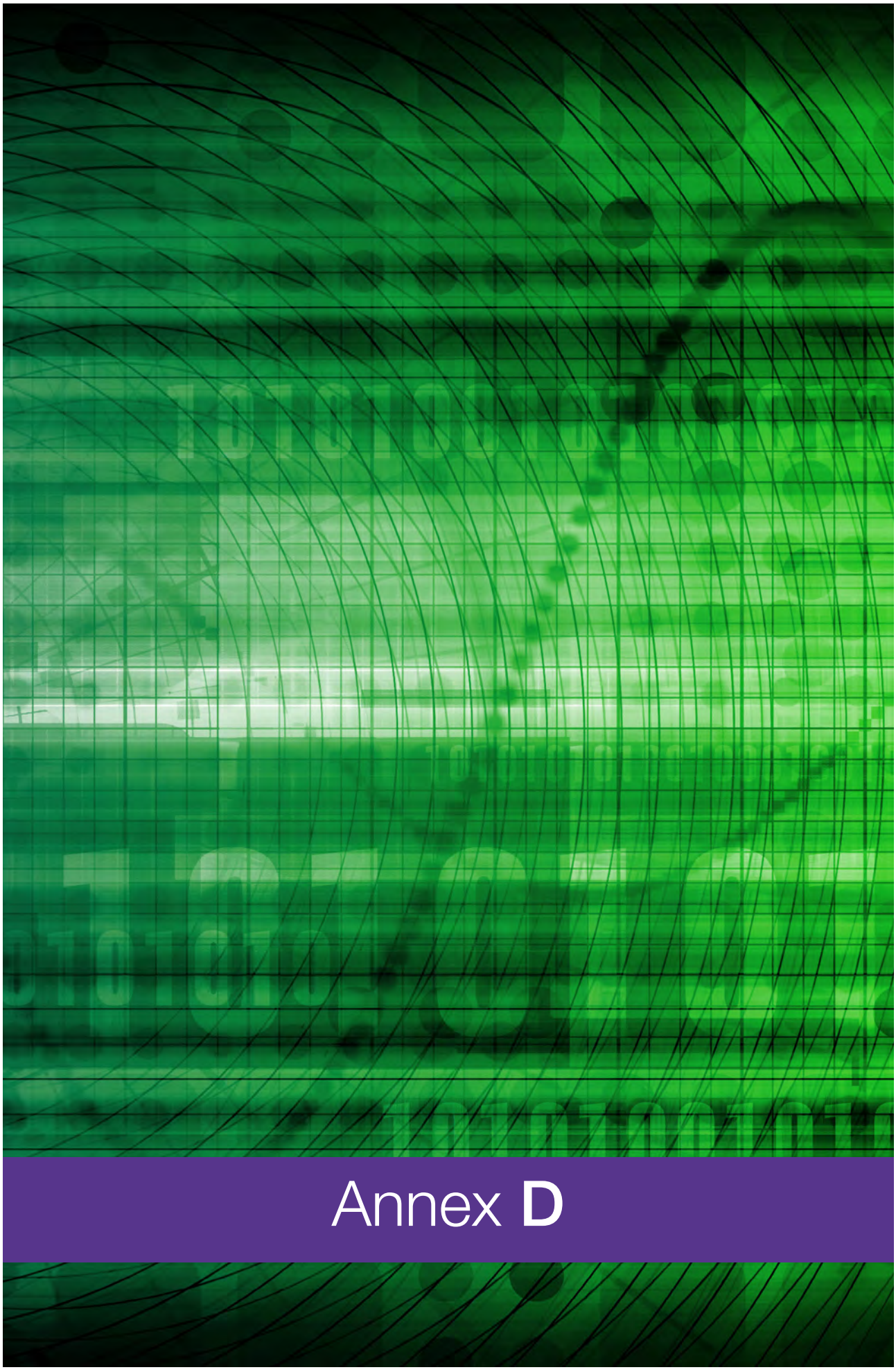
A fraud estimate takes a statically valid sample of payments within an area and tests them for incidents of fraud. The level of fraud found is then extrapolated across the rest of the population. The extrapolation will often be in a range, with a degree of certainty.

It should be noted that:

- Fraud measurement exercises often look at discrete areas – they do not cover the whole of an organisations spending or income;
- Fraud measurement exercises often identify fraud and error (irregularity) as opposed to pure fraud. This is because the difference between fraud and error is intent, and to establish that an incorrect payment or claim has been done intentionally requires investigation. In some measurement methodologies, proxies are used for intent (for instance, if a certain action is more likely to be intentional than an error then it is considered fraud). However, it should be noted that this approach has a degree of uncertainty around it;
- Measurement exercises produce a range of likely levels of fraud. For instance, measurements of the level of fraud and error within the benefits (social security) system in the United Kingdom lead to an estimate that fraud and error levels are between 1.8% of expenditure and 2.5% of expenditure. In some instances, the midpoint of these estimates are taken as the most likely level. This simplifies the communication of the results. However, the degree of uncertainty should be recognised.

Unknown Fraud

When undertaking a fraud measurement exercise, a limited number of fraud risks or scenarios, and their associated indicators have to be focused on. Some, more sophisticated, frauds are very difficult to identify through fraud measurement exercises and some fraud risks may be left out. As such, it is likely that there will be some, undetected, unknown, not estimated residual level of fraud in a system that has an estimates and detected levels. This is not possible to measure, but should be acknowledged.



Annex **D**

Annex D - Bibliography

Agnew DJ, Pearce J, Pramod G, Peatman T, Watson R, et al. (2009). *Estimating the Worldwide Extent of Illegal Fishing.*
→ https://doi.org/10.1371/journal.pone.0004570

Association of Certified Fraud Examiners (2018). *Report to the Nations – 2018 Global Study on Occupational Fraud and Abuse.*
→ https://s3-us-west-2.amazonaws.com/acfepublic/2018-report-to-the-nations.pdf

Australian National Audit Office (August 2018). *Annual report 2018-19.*
→ https://www.anao.gov.au/work/annual-report/anao-annual-report-2017-18

Bertram I. Spector (2005). *Fighting Corruption in Developing Countries: Strategies and Analysis.* Bloomfield, CT: Kumarian Press.

Button, M, Chris Lewis and Jacki Tapley (April 2012). *Not a victimless crime: The impact of fraud on individual victims and their families.*
→ https://link.springer.com/article/10.1057/sj.2012.11

Cross, Cassandra, Russell G Smith and Kelly Richards (May 2014). *Challenges of responding to online fraud victimisation in Australia.*
→ https://aic.gov.au/publications/tandi/tandi474

Dobel, JP. (2018). *Public Leadership Ethics: A Management Approach.* Routledge

Ganzini, Linda, B McFarland, Joseph D Bloom (February 1990). *Victims of fraud: Comparing victims of white collar and violent crime.*
→ https://www.researchgate.net/publication/20971949_Victims_of_fraud_Comparing_victims_of_white_collar_and_violent_crime

International Public Sector Fraud Forum (February 2019). *Guide to Managing Fraud for Public Bodies.*
→ https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/778306_GuideToManagingFraudForPublicBodies.pdf

Murphy, P., & Dacin, M. (2011). Psychological Pathways to Fraud: Understanding and Preventing Fraud in Organizations. *Journal of Business Ethics, 101(4), 601-618.*
→ www.jstor.org/stable/41475922

National Fraud Authority, United Kingdom (2009). *Fraud typologies and victims of fraud.*
→ http://www2.port.ac.uk/media/contacts-and-departments/icjs/ccfs/Fraud-typologies-and-victims.pdf

Pascoe, T., Owen, K., Keats, G. and Gill, M. (2006). *Identity Fraud: What about the Victim.* Leicester, UK: Perpetuity Research and Consultancy International.

PriceWaterhouseCoopers (February 2014). *Fighting fraud in the public sector III.*
→ https://www.pwc.com.au/pdf/fighting-fraud-feb151.pdf

PriceWaterhouseCoopers (June 2011). *Fighting Fraud in the Public Sector.*
→ https://www.pwc.com/gx/en/psrc/pdf/fighting_fraud_in_the_public_sector_june2011.pdf

Spalek, B (May 1999). *Victims of fraud: Comparing victims of white collar and violent crime.*
→ https://journals.sagepub.com/doi/10.1177/026975809900600304

Titus, Richard and Angela R. Gover (January 2001). *Personal Fraud: The Victims and the Scams.*
→ https://www.researchgate.net/publication/257656023_Personal_Fraud_The_Victims_and_the_Scams

UK Cabinet Office. *Professional Standards & Guidance for the 'Fraud Risk Assessment.'*
→ *For more information on Professional Standards & Guidance for the 'Fraud Risk Assessment' please contact* GCFP@cabinetoffice.gov.uk

UK Cabinet office (2018). *Cross-Government Fraud Landscape 2018.*
→ https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/764832/Cross-GovernmentFraudLandscapeAnnualReport2018.pdf

UK Cabinet office (2017). *Cross-Government Fraud Landscape 2017.*
→ https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/642784/2017-09-06_Cross_Government_Fraud_Landscape_Annual_Report_final.pdf

Winbourne, Svetlana (2005). *Fighting Corruption In Developing Countries in Environment and Natural Resources.* Chapter 7, p. 104, in: Spector, Bertram I. (ed.), 2005. Bloomfield, CT: Kumarian Press.