COUNTER FRAUD CENTRE
Tauārai Hara Tāware

Low Friction Countermeasures for Fraud Prevention in Times of Crisis

May 2023

Table of contents

1 Introduction 2

1.1 Overview 2

2 Low friction Countermeasures 3

2.1 Include fraud clauses 4

2.2 Recovery and debt management 5

2.3 Parameters and limits 6

2.4 Avenues for reporting fraud 7

2.5 Governance and oversight 8

2.6 Public/private partnerships 9

2.7 Account Protections 10

2.7 Remediate compromised identities 11

1 Introduction

This is the first of two guides that provide examples of countermeasures that can be used to support the policy and delivery teams to reduce significant fraud and corruption risks.

This guide is focused on the third principle of fraud control in disaster management, namely: *The business and fraud control should work together to implement low-friction countermeasures to prevent fraud risk where possible,* by providing examples of low-friction countermeasures that your organisation can implement or improve.

The second guide is focused on the fourth principle of fraud control in disaster management, namely: *Carry out targeted post-event assurance to look for fraud, ensuring access to fraud investigation resource*, by providing examples of how to use data to support post-event assurance activities.

For more information about effective control of fraud in disaster scenarios visit https://sfo.govt.nz/counterfraud/cfc/resources/guides-and-factsheets/fraud-prevention-in-times-of-crisis

1.1 Overview

This guide contains high level information on **eight low-friction countermeasures**. Not all countermeasures are appropriate for all organisations. Using this guide, practitioners will be able to determine whether it is appropriate to adopt the countermeasure based on their organisations risk exposure and tolerance.

All nine countermeasures include a description of the countermeasures followed by six sections.

- *‘Why this is important in a crisis’* provides context to the reasons the countermeasure helps to reduce the risk of fraud during times of disaster response and recovery.
- *‘More about this countermeasure’* provides additional information about the countermeasure.
- ‘Consideration for implementation’ provides examples of risk associated with the implementation of the countermeasure.

2 Low friction countermeasures

This guide contains **eight low-friction countermeasures** and should not be considered an exhaustive list of all detection countermeasures. A low-friction countermeasure is a control which sets the balance between the need to ensure fast distribution of funds to where they are needed and the requirement to keep fraud risk low, ensuring that monies do get to where they are required.

Use this guide to:

- consider whether an organisation is exposed to fraud risks which these countermeasures mitigate against
- identify whether these countermeasures have been or should be in place to mitigate these fraud risks

2.1 Include Fraud Clauses

Include clauses about fraud and privacy in applications, disclaimers and contracts to provide protection and/or redress for your organisation

Why this is important in a crisis

In disaster situations organisations are required to get the help and funds to those who need it. It's often not possible to manually check the accuracy of claims due to the high volume of claims. Organisations are therefore reliant on more automated processes to provide support to those in need.

Fraud clauses can enable entities to collect, use and share personal information that can be used for fraud assurance checks and data matching to identify fraudulent or erroneous claims.

Fraud clauses can be a way in which agencies communicate that they may take civil or criminal action where suspected fraud is identified. This communication can serve as a deterrent for opportunistic fraudsters.

More about this countermeasure

Appropriate clauses in applications, disclaimers or contracts can:

- set out applicants' obligations – for example, providing accurate information, or having fraud arrangements in place (for service providers and business grants recipients)
- place clear limitations on the use of funding, governments assets or information
- inform applicants of the consequences of providing false information or committing fraud
- obtain consent to use information for fraud assurance checks and data matching to ensure the integrity of the relief funding.

Considerations for implementation

Fraud clauses have legal implications. Get legal advice before writing any fraud clause, to ensure it is enforceable.

Fraud clauses should be built into upfront disclaimers or contracts – they should be clearly visible and used with a consent box.

2.2 Recovery and debt management

Put in place arrangement to allow for the recovery of money incorrectly paid because of fraud or error.

Why this is important in a crisis

Disaster scenarios often does not allow for upfront controls to be implemented and reliance is placed on post event activities to detect fraudulent or erroneous payments and to recover the money.

Recovery arrangements makes it possible to recover money as a result of incorrect payments, grants, loans, or subsidies.

Seizing assets and recovering funds wrongly paid due to fraud can act as a strong deterrent to fraud.

More about this countermeasure

New Zealand public sector agencies can use a variety of methods to recover money incorrectly paid because of fraud or error, for example:

- **clauses to recover or claw back money** are legally binding provisions that enable entities to demand repayment if a grant or payment is paid in error, or if a person or entity breaches a specific use clause. Recovery arrangements can be included in applications, disclaimers or contracts or provided through legislation.
- **debt recovery powers in legislation** are powers to garnishee tax returns (a garnishee is a third party instructed by legal notice to pay money to settle a debt or claim). This power incudes making deductions from future payments or departure prohibition orders.
- **confiscation of criminal assets** includes only disposing of assets after the confiscation proceedings have ended.

Considerations for implementation

Recovery arrangements or clauses have legal implications. Get legal advice before writing them to ensure they are valid and enforceable.

2.3 Parameters and limits

Set specific parameters and limits, such as the maximum amount that can be claimed or paid, or a threshold for applications before additional scrutiny is applied.

Why this is important in a crisis

It is likely that manual verification of applications will be impractical due to the number of applications and the speed at which the funding needs to be delivered.

It may be possible to conduct targeted verification processes on applications that fall outside of pre-determined parameters and limits and limiting the extent of fraudulent or erroneous transactions before they are completed.

Alternatively post event assurance activities can be prioritised by starting with applications that fell outside of pre-determined parameters and limits.

More about this countermeasure

Setting specific parameters and limits allows applications to be streamlined, while also providing some assurance around high-risk applications.

Where possible, a system should not enforce parameters or limits such as:

- the system will not allow payments to be paid above a certain limit
- particular items/payments cannot be claimed together.

This countermeasure can also be boosted by sharing data across New Zealand public sector agencies to determine whether applicants are improperly claiming across multiple programmes/subsidies.

Considerations for implementation

Exceeding a parameter or limit does not necessarily indicate suspected fraud; certain applicants may have legitimate reasons for claiming above the threshold. The countermeasure may only limit applications within one programme or policy.

New Zealand public sector agencies also need to watch out for a person or business making claims across multiple programmes.

2.4 Avenues for reporting fraud

Give employees, individuals and businesses safe avenues for reporting suspected fraud or other criminal behaviour.

Why this is important in a crisis

Providing a clear avenue for reporting ensures that suspicious behaviour, which might otherwise be overlooked, can be identified and investigated.

More about this countermeasure

A tip-off is the most common way that fraud is detected. Clear and confidential processes should be in place to support employees, individuals and businesses to lodge tip-offs.

Considerations for implementation

To be effective, employees, individuals and businesses must have confidence in any tip-off or reporting process. Two factors in particular that discourage reporting are:

- a lack of confidence that the organisation would act in respect of a report
- a lack of confidence that the organisation had adequate protections in place for those who report

This countermeasure relies on public sector agencies having systems in place to receive tip-offs (including from employees under the Protected Disclosures Act 2000) and the resources to respond to tip-offs and protected disclosures. In a high triage process, some tip-offs may not be prioritised.

The information that public sector agencies collect from tip-offs can also be a limitation. For good reasons, tip-offs are often provided anonymously. Yet they may also provide insufficient information to act on

2.5 Governance and Oversight

Establish and maintain good governance, accountability and oversight over processes, decision making and programme risks.

Why this is important in a crisis

Governance, accountability and oversight can be diminished when disaster relief and recovery measures are being designed and delivered at pace. Organisations must do what they can to maintain oversight of processes, decision making, and risk in this environment.

Good governance, accountability and oversight increases transparency and reduces opportunities for fraud. Good governance also includes completing a detailed fraud risk assessment.

More about this countermeasure

Fraud risk assessments should identify who is accountable for managing the identified fraud risks and vulnerabilities.

Project reporting requirements and governance arrangements should also exist to increase transparency of, and accountability for, project outcomes, including fraud losses

Considerations for implementation

Providing effective oversight and accountability in a fast-paced environment following a disaster or emergency is inherently harder.

Some organisations may need to quickly onboard large numbers of new employees or redeploy employees to assist with the disaster relief and recovery response. This can disrupt the established reporting lines and oversight. So, governance and oversight arrangements must also adapt to new conditions.

Managers should ensure that they are still communicating how to identify red flags, discussing fraud risks, and communicating how to escalate issues during periods of disruption.

2.6 Public/private partnerships

Work with established and trusted private sector partners to share capability, information and intelligence.

Why this is important in a crisis	Strategic partnerships with the private or not-for-profit sectors are important for all New Zealand public sector agencies but may be especially needed to rapidly roll out disaster relief and recovery programmes that have large numbers of applicants and payments. These partnerships support organisations to share information and intelligence to prevent, detect and respond to fraud.
More about this countermeasure	Where possible and permissible*, work with well-established and trusted partners such as public sector agencies, reputable non-government organisations and established businesses to deliver services. This collaboration can often be a lower risk option. Collaborate as much as you can with trusted partners to share capability, information and intelligence to prevent and disrupt fraud. *Some structures such as trusts have specific operational parameters that they can operate it in. Organisations should confirm that the trust is operating in line with the trust deed and has proper processes in place for the trustees to fulfil their obligations.
Considerations for implementation	Effective data-sharing arrangements rely on data availability, data quality, and authority to share data. Some privacy provisions may not allow reciprocal information sharing. Consult your Legal Services team to explore your legal frameworks. If restrictions exist, look for opportunities to share information where possible.

2.7 Account Protections

Protect client accounts from unauthorised access and changes.

Why this is important in a crisis	Protections for client accounts are important because criminals could use compromised personal identifying information to access victims' accounts in order to fraudulently claim or divert payments. Protecting client accounts from unauthorised access and changes can reduce the risk of identity compromise, payment hijacking and insider threat.
More about this countermeasure	Protections should apply across multiple channels, such as telephone and online channels. Preventing unauthorised access and changes to accounts will assist in preventing fraud or further identity compromise. Protections for account changes should also apply to internal processes to minimise the threat of unauthorised access and changes to client accounts by trusted insiders. Communicate and limit how and when a client's account details can be accessed and changed. Protections can include two-factor authentication, identity authentication, automatic notifications to clients about account changes, change management processes, and segregation of duties..
Considerations for implementation	This countermeasure does not prevent fraudulent accounts being created. New Zealand public sector agencies cannot stop a person or business losing or exposing their own identity information or account credentials. New Zealand public sector agencies can take active steps to educate their clients about the risks. Some measures rely on private sector organisations to deliver support to clients. These measures will be susceptible to fraud if those organisations fail to adequately protect their clients' accounts.

2.8 Remediate compromised identities

Put procedures in place to identify, alert and assist victims of identity fraud.

Why this is important in a crisis

Remediating compromised identities is important for all public sector agencies but will particularly support those who are rapidly rolling out programmes that have large numbers of applicants.

In a disaster environment, fraudsters will seek to steal identity information or use already compromised information to obtain access to funding. Alerting other agencies and the victim of identity theft can help stop the continued use of the victim's identity information and minimise the impact of fraud.

More about this countermeasure

New Zealand public sector agencies dealing directly with the public should put processes in place to identify and remediate these two circumstances:

- individuals or businesses have had their identities stolen and misused to apply for government programmes or grants
- individuals or businesses have had their identity leaked, stolen or inappropriately accessed.

Public sector agencies should also ensure they have procedures in place to assist individuals or businesses to recover and restore their identity, or support organisations such as ID Care, which provides free support to individuals and businesses that have had their identity compromised.

Public sector agencies should also alert other relevant agencies who may be engaging with those same individuals or businesses who have had their identities compromised.

Considerations for implementation

Public sector agencies cannot stop individuals or businesses losing or exposing their own identity information. Agencies may also be able to detect and limit identity theft.

COUNTER FRAUD CENTRE

Tauārai Hara Tāware