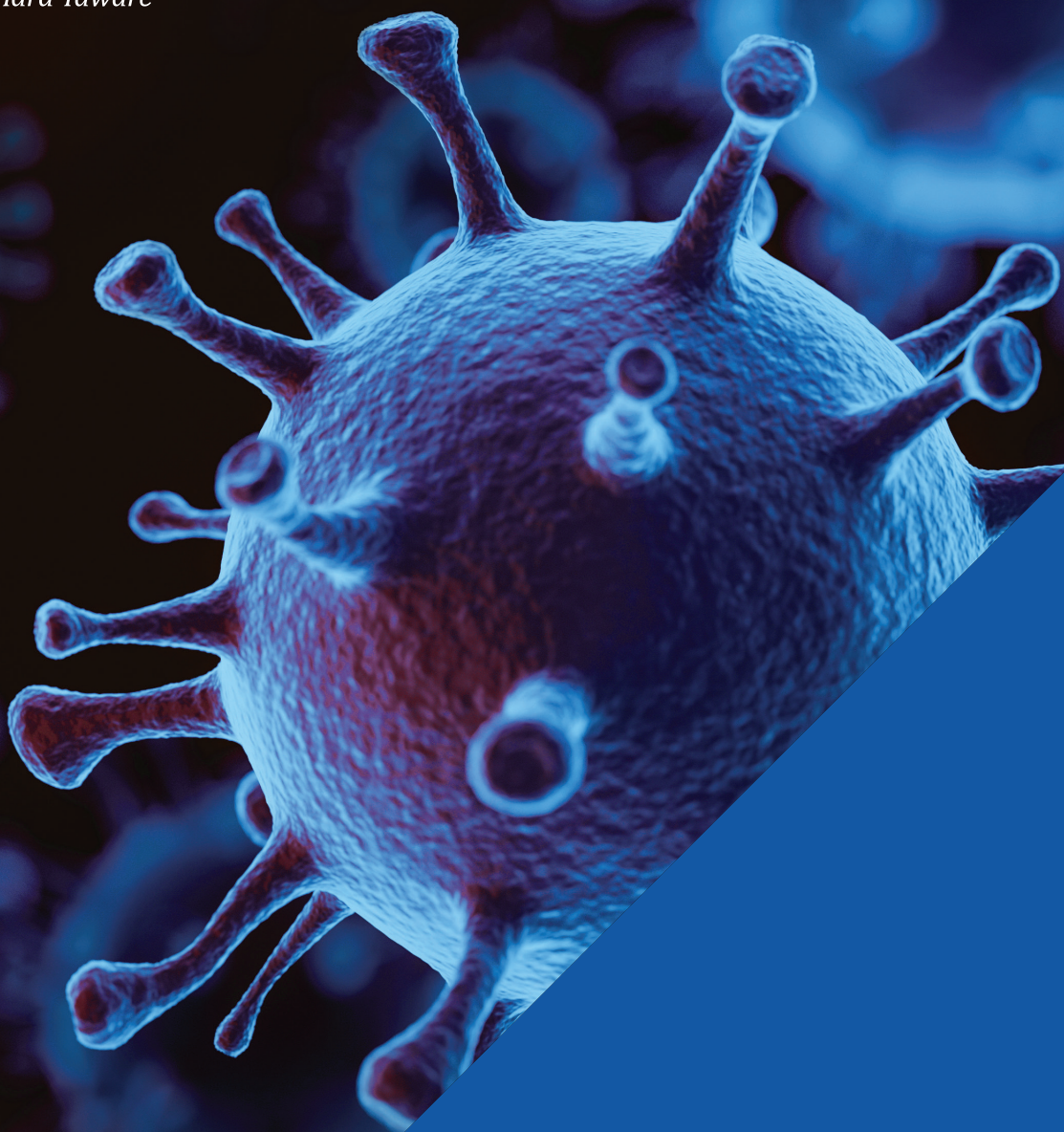




SERIOUS FRAUD OFFICE

Te Tari Hara Tāware



COUNTER-FRAUD

TOOLKIT

**FOR COVID-19
RELIEF RESPONSES**

COUNTER-FRAUD TOOLKIT

FOR COVID-19 RELIEF RESPONSES

In emergency or disaster recovery situations such as the COVID-19 pandemic, it is vital that the government can distribute relief funding as quickly as possible. This includes providing support and services to those in need and rebuilding communities and infrastructure. However, fraud can significantly undermine these efforts if it is not addressed.

The provision of emergency relief and associated services by government has an inherently high risk of fraud (both internal and external) because the speed at which it must be delivered will often compromise normal controls. New Zealand's COVID-19 relief response ranges from the direct payment of funds under the wage subsidy scheme, through to the provision of a specific emergency service such as repatriation, which involves procuring the services of third-party providers to assist. Given the breadth and speed of the response, it is a prime target for those

The key goals for counter-fraud measures in an emergency management context are:

- Rapid design and delivery of upfront low friction checks, which don't slow down the delivery of relief funds; and
- Where upfront controls are not possible, designing post-event assurance delivered at the right time and in the right way.

seeking to make gain at the expense of others. At the same time, it is not possible or appropriate to put in place measures that will remove all risk of fraud, as that will prevent or at least slow the funds getting to where they need to go.

GUIDING PRINCIPLES

Agencies responsible for the design and administration of COVID-19 relief programmes should:

1. Accept there is an inherent risk of fraud and it is likely to happen.
2. Where possible, integrate fraud control personnel into the policy and process design to build the awareness of fraud risks.
3. Work together with fraud control personnel to implement low friction countermeasures to prevent fraud where possible.
4. Carry out targeted post-event assurance to check for instances of fraud.
5. Be mindful of the shift to longer term services (from emergency payments) and revisit the control framework at this point.

FURTHER ASSISTANCE

If you require further information about this toolkit, if you would like assistance in relation to the design, implementation or operation of a specific relief programme or if you wish to report any instances of suspected fraud in the context of COVID-19 relief, then please contact the Serious Fraud Office at counterfraud@sfo.govt.nz.

CONTEXT

We are aware from our international counterparts that other countries have seen a significant rise in fraudulent activity generally as a result of COVID-19. This has reflected both the opportunistic targeting of those in need, as well as the redeployment of established criminal activity to defraud government relief programmes.

This toolkit is intended to be read as a more detailed supplement to the high-level guidance contained in our 'Counter-fraud guidance for Covid-19 relief responses' document. It will focus on steps that can be taken by individual agencies and the public sector more generally to mitigate the risk of fraud in the context of government relief efforts.¹ It is based on the Serious Fraud Office's expertise in investigating and prosecuting public sector fraud, as well as from our membership of the International Public Sector Fraud Forum where we have access to the collective experience of our Five Eyes partners. That experience includes issues that have already arisen in the context of these jurisdictions' COVID-19 responses, as well as previous emergency relief programmes associated with the recent Australian bush fires and the Grenfell Towers disaster.

It should also be noted that the steps detailed below relate to measures that can be implemented or addressed in relatively short order given the current emergency response context. In order for agencies to achieve a long term and sustainable counter-fraud programme, more fundamental measures including but not limited to integrity checks, specialised staff counter-fraud training, tailored data analytics programmes, detailed agency specific fraud risk assessments, pressure testing of counter-fraud controls, and fraud prevention measurement, would all be recommended.

In addition, some of the steps outlined in this toolbox relate to addressing risk at the early stages of the relief delivery process, such as the design phase. We are conscious the COVID-19 relief programme is already underway, so we acknowledge it may not be possible to take all the steps outlined below given the pace at which the response has had to proceed.

Finally, the relevance of these steps will depend on the specific circumstances of the relief or service being provided and a case by case assessment of their applicability will need to be made. Their adoption will not remove the risk of fraud, but they do provide a framework for an appropriate mitigation strategy.

¹ The SFO is aware that in response to COVID-19, fraudsters are targeting members of the public more directly. Methods seen to date in other jurisdictions have included online scams, bank account fraud, investment fraud, the sale of counterfeit or non-existent health products and the offer of fake services such as goods delivery. This is a separate issue which involves a different set of mitigation and prevention strategies.

CONTENTS

Updated 29 May 2020

ENSURING AWARENESS 03

- Clear and proactive communications strategy
- Train staff to identify and report fraud
- Tip-offs and reporting fraud

DESIGN AND GOVERNANCE 04

- Policy and process design
- Use existing systems and criteria where possible
- Existing decision-making processes, delegations and controls must be maintained
- Protective clauses
- Work with well-established, tried and tested partners where possible

PAYMENTS 06

- Ensure payments are processed by staff with appropriate oversight
- Requests or claims are randomly allocated for processing
- Ensure easy repayment

REAL-TIME AND POST-EVENT ASSURANCE 07

- Use bank account data
- Automatic notification of high-risk transactions
- Identity is appropriately authenticated for each interaction
- Data protected from manipulation or misuse
- Collaboration, data matching and information sharing with strategic partners
- Data analytics
- Post-fraud assurance
- Internal fraud

ENSURING AWARENESS

Clear and proactive communications strategy

A clear and proactive communication strategy from relevant agencies and the public sector generally is required so the public know scrutiny will be applied to the payment of relief funds (either at the time of payment or at a later point) and anyone who is found to have taken advantage of COVID-19 to engage in fraudulent conduct will be held to account.

It is essential that both established criminals and opportunists do not perceive the government's COVID-19 response and its commitment to provide relief funds as a signal that there will be a tolerance for fraud.

The government's commitment to provide relief funds to those in need is not a signal that there will be a tolerance for fraud.

Train staff to identify and report fraud

Fraud is more likely to happen in organisations where staff are not aware of what fraud is, cannot identify the red flags that would signal its presence or do not know what to do if they suspect it. The ability of agencies to provide comprehensive fraud awareness training to all staff dealing with COVID-19 relief will be limited by the short window of time that exists to get the funding delivered. However, subject to this practical constraint, it is vital that relief delivery staff receive some form of fraud detection training, as well as regular and ongoing messages on fraud awareness to help them to identify fraud and to know how to report it.

Tip-offs and reporting fraud

As an associated measure, there needs to be a clear channel for those within agencies and amongst the general public to report fraud, including the making of Protected Disclosures.

For most agencies associated with delivering relief funds, this should simply involve drawing attention to methods of reporting that already exist. If a dedicated line for reporting fraud does not exist, it must be established immediately. It can take many forms including an anonymous phone line, an online form (internet and intranet) or an email address. The key feature is that it must be accessible and easy to use.

Once a reporting line for fraud is in place it must also be publicised. Reporting lines are ineffective if people don't know they exist. The prominent presence of a fraud reporting line reinforces to agency staff that a more pronounced focus on speed of delivery does not mean fraud awareness can be compromised. For the general public, it lets them know that law enforcement agencies who focus on financial crime remain 'open for business'.

DESIGN AND GOVERNANCE


Policy and design process

At the outset of any response, when policy and delivery areas are developing emergency management processes, where possible there should be experienced fraud personnel involved to analyse the policies and processes as they are developed. Their role is to identify how the system could be defrauded (ideally by carrying out a fraud risk assessment), to record this and to communicate it to the key responsible leads. It should be part of the role of the leader of the emergency management activity to ensure effective fraud control resource is identified and embedded in the policy and design process.

It is important that any risk and mitigation strategies identified are shared across government. This could take the form of:

- Connecting shared risk and control owners across agencies.
- Facilitating or supporting fraud risk workshops to identify cross-agency and measure specific risks and controls.
- Developing and distributing a standardised risk assessment template and guidance for agencies to conduct risk assessments for individual relief measures.
- Identifying and advising government and agencies of cross-agency gaps and the highest fraud risks for COVID-19 relief measures.

It is crucial to note a fraud risk assessment (for COVID-19 or more generally) is never complete. It is an ongoing exercise and the risks and mitigations identified must constantly be revisited to scan for new threats and risks and to assess whether the responses remain relevant and appropriate.



Fraud risk assessment is an ongoing exercise.

Use existing systems and criteria where possible

In emergency management situations, systems, processes and policies (including the criteria for services and payments) are created at pace and carry higher levels of uncertainty and change than standard policies and processes. Those leading the response can also struggle to resource the recording of criteria and processes.

An effective way to mitigate the enhanced risk of fraud this brings can be to use existing systems and criteria for payments and services. For instance, services to restore affected infrastructure could use existing processes for the restoration. Equally, support of those experiencing hardship as a result of a crisis should, where possible, be linked to eligibility criteria for other public services.

Existing decision-making processes, delegations and controls must be maintained

The process and delegations for decision-makers to authorise payments must be clearly defined and documented in specific instruments or instructions. Similarly, policies relating to conflicts of interest and declarations of interests (including gifts and hospitality) must be clearly set out and communicated.

For most agencies, these processes already exist but there is a temptation to short-cut them in the context of an emergency response. The reality is that emergency conditions actually heighten the need for such processes to be strictly observed. Keeping to these rules will have little or very limited impact on the speed of relief delivery, but a failure to observe these processes on the basis that emergency responses require (or at least justify) a relaxation of standards will likely have two effects:

- It sends a signal that controls have been relaxed and there are opportunities for fraud.
- It will make post-event assurance and quality checks much more difficult as there will not be a proper audit trail to follow.

Protective clauses

Agreements or documentation that record the terms and conditions on which relief is to be given can contain clauses that provide protection and/or redress for the government. For example:

- A claw-back clause can be included which immediately entitles public bodies to demand repayment if relief funding is paid in error, if a specific usage clause is breached or if any details given are false. This provides a fast track process for getting funds back without a protracted legal process.

- Similarly, a fraud clause sets out the obligations of the applicant to provide accurate information for the purpose of making an application and assessing the applicant(s) entitlement for a particular relief scheme. It could set out what might happen if the applicant provides false or misleading information (automatic claw-back), and how their information will be used.
- In terms of use of information, for Privacy Act purposes, the clause could go on to record the recipient's agreement that their details can be shared for the purposes of fraud assurance checks and data matching to ensure the integrity of the relief delivery.

Work with well-established, tried and tested partners where possible

When engaging with third party partners to deliver emergency management, there can be limited time to carry out upfront due diligence or fit for purpose checks to the extent that would be expected in other circumstances. This can lead to a higher risk of fraud as the organisation may be working with partners that have very limited assurance.

To a certain extent, this risk can be mitigated by using tried and tested partners who have already been through due diligence processes. This does not however remove the risk of fraud, as fraud is committed by individuals, not organisations, and there is still a risk that either individuals in the organisation will be motivated to commit fraud or people will join the organisation and commit fraud.

PAYMENTS

Ensure payments are processed by staff with appropriate oversight

Allowing a large number of staff to process requests for relief funds increases the risk that someone may deliberately process fraudulent claims or be coerced into doing so. Limiting access to processing payments to specialised users during emergency responses can reduce this risk.

Functionality within systems should also be limited/controlled by user permissions, which are assigned to users based on specific business needs. High-risk functions (such as payments over a certain level) should also be limited to specialised users with all access being auditable. Other specific restrictions could include users being blocked from accessing their own programme record.

Requests or claims are randomly allocated for processing

The risk of a staff member using their position of trust to process fraudulent requests or claims for themselves or another person or entity can be mitigated by ensuring requests or claims for relief are randomly allocated to staff for processing. This removes the option for staff to select which claims to process. Where possible, staff and contractors should also be rotated in and out of roles or contracts to avoid familiarity.

Ensure easy repayment

The purpose of this toolkit is to address the risk of public funds being lost at a time when New Zealand is focused on economic recovery and where every dollar counts. Accordingly, in addition to ensuring that fraud risk is minimised, where entities or individuals wish to make repayments of government relief funds that they have received, agencies should make this process as easy as possible. This includes situations where a payment was made in error, or where circumstances have changed meaning that the recipient is no longer eligible, or otherwise not in need of the payment.

Agencies concerned with the provision of any form of COVID-19 relief should therefore:

- Ensure there is clear communication of how eligibility for a particular government programme works. This will allow willing compliers to assess their entitlement on an ongoing basis. If the rules around entitlement change (which is to be expected in the context of a fast-moving pandemic response) then these changes must be clearly communicated.
- If a recipient does wish to make repayment, then there should be an ability to do so quickly and electronically in a small number of steps through the relevant agency's website. Instructions to make repayment must be clear and obvious. This should be accompanied by a telephone helpline option where users are having difficulty with electronic access.

REAL-TIME AND POST-EVENT ASSURANCE

Use bank account data

Multiple data sets already exist across government where valid bank account numbers are used to make or receive payments for a range of purposes. This includes direct debit instructions and bank details held for benefit payments and tax refunds.

Fraud is less likely to be present where payment accounts are long standing and have already been subject to some form of verification. Data matching between agencies can ensure the bank account information that is already held is used as a further check on the integrity of the process. For example, this data could be used to validate whether a bank account, put forward to receive relief payments, in fact belongs to the claimant individual or business, lessening the risk that an incorrect or fraudulent account is paid.

If the collection of data is high quality, post-event assurance will be more efficient.

Automatic notification of high-risk transactions

A common type of emergency relief fraud relates to the use of another person's identity to obtain benefits. This can be mitigated by having system generated notifications sent to known contact locations for high-risk transactions, such as:

- access to online accounts
- submission of claims or requests
- changes to contact details
- changes to bank accounts
- outcomes of claims or requests.

These notifications may alert customers or staff to fraudulent activity. Resources and technology will dictate what type of notifications are possible, but some examples of this type of countermeasure used to date include:

- Customers receive an SMS notification to confirm receipt of a new claim.
- Customers or providers are automatically notified via email that their bank account details have been updated.
- Customers are automatically notified when their online account is accessed.
- Regular payment statements are automatically sent to recipients.
- Customers are automatically notified when their address or contact details are amended.

REAL-TIME AND POST-EVENT ASSURANCE contd.

Identity is appropriately authenticated for each interaction

All relief programmes will require some level of mandatory information to support the initial claim or request, such as copies of primary and secondary identification (passport, birth certificates, driver's licences etc). The level and nature of detail required for each programme will differ, but once settled it should be applied consistently and without exception.

Those managing the response should retain records of payments, services delivered and the evidence provided to demonstrate that services were delivered, or individuals were eligible for the services or payments. If the collection of data is consistent and of a high quality this will make post-event assurance more efficient (including allowing the effective use of data analytics noted below) and will act as a deterrent to those who would commit fraud.

Once a claim is accepted there is a need for identities to be authenticated for each interaction by testing the credentials supplied by the person making the claim. Some examples of this type of countermeasure used in the context of emergency relief include:

- All customers or providers (those third-party organisations tasked with supporting relief delivery) must pass an identity authentication check prior to servicing.
- Customers or providers must pass a two-factor authentication to access their online account.
- Where relevant, customers must enter a unique PIN to access a mobile app.

Data protected from manipulation or misuse

Where possible, protections should be put in place to prevent data from being manipulated or misused and to ensure the relief programme's source code or audit logs cannot be altered in production environments.

Some specific examples of this type of countermeasure include:

- Pre-fill data cannot be changed on forms.
- Reports are 'read only' to prevent manipulation.
- Data is coded directly into systems and cannot be manually altered.
- Updates to production data are restricted by system parameters.
- A system's source code cannot be altered outside a prescribed change management process.
- Audit logs cannot be altered.

REAL-TIME AND POST-EVENT ASSURANCE contd.

Collaboration, data matching and information sharing with strategic partners

Fraud is more likely to occur where relief payments (and associated assurance measures) are taken by individual agencies without the support of other relevant parts of the public sector. Collaboration can occur through strategic partnerships such as government agencies, committees, working groups and taskforces sharing capability, information and intelligence, in order to prevent and disrupt fraud.

Examples of this type of countermeasure include:


- Partnerships with other government agencies, committees, working groups and taskforces to share information and data.
- Working with policy agencies to contribute to programme design and implement legislative, policy, and procedural change.
- Collaboration with international counterparts to share expertise, improve processes and prevent fraud.

At a more specific level, collaboration between agencies can allow information sharing and data matching to occur whereby data is automatically matched with one or more sources to obtain or verify details relevant to the request or claim. The purpose of this process in the COVID-19 context would be to identify inconsistencies that may indicate fraud.

The current approved information sharing agreements and matching provisions are listed in Schedules 2A and 3 of the Privacy Act respectively² and their terms must be strictly adhered to. It is also of note that emergency information sharing powers have been triggered by our Civil Defence National Emergencies (Information Sharing) Code 2013. As a consequence of this code, some of the usual Privacy Act restrictions on sharing and disclosure of data

by government agencies do not apply.³ However, it should be noted the application of this Code is limited in time to 20 days after a state of emergency has ceased to be in effect.

As noted above in relation to protective clauses, obtaining consent as part of the payments process may also further assist in ensuring compliance with Privacy Act obligations.



Collaboration between agencies can help identify inconsistencies that may indicate fraud.

Data analytics

At the payment stage, a basic step would be to ensure duplicate requests, claims or records are prevented, identified and corrected.

As a post-event step (to avoid slowing down the relief payment process), the use of more sophisticated data analytics to detect error and fraud is appropriate. As noted above, the extent to which data analytics processes can be applied depends on the quality and consistency of the data obtained at the time of service delivery.

Some examples of this type of post-event countermeasure include:

² See also: <https://www.privacy.org.nz/privacy-for-agencies/information-sharing/>

³ For further detail see: <https://www.privacy.org.nz/the-privacy-act-and-codes/codes-of-practice/civil-defence-national-emergencies-information-sharing-code-2013/civil-defence-national-emergencies-information-sharing-code-2013>

REAL-TIME AND POST-EVENT ASSURANCE contd.

- Profiling common fraud methodologies against programme data.
- Risk scoring based on recipient characteristics and payment types.
- Analysing trends and patterns in programme data, for example, increased fraudulent behaviour via online channels.
- Spatial analysis to identify claiming patterns and anomalies, for example, claims for relief payments outside affected areas.
- Washing large data sets together to identify suspicious activity.

Post-fraud assurance

The extent to which upfront and preventative counter-fraud measures can be implemented will be limited. Therefore, it is important that post-event activity is undertaken in as timely a fashion as possible to establish whether the fraud risks identified and understood came to pass. Using any fraud risk assessment created during the policy and process design, the agency should carry out post-event assurance work to check for instances of fraud.

Agencies should also be mindful of the shift from emergency payments to more long-term services. This change provides an opportunity to revisit, test and if necessary revise the control framework – especially where large sums are invested.

There will come a point in the COVID-19 relief delivery when the initial time-pressured response comes to an end and more systematic investment starts for longer term services and support (for example, moving into the recovery phase). If this is led by the same organisation or team that led the emergency response, there is a risk that the short-term processes and culture built by the team developing the policies and processes can last longer than is necessary. This can unnecessarily increase the risk of fraud and corruption in these less time pressured emergency management situations.

Those leading emergency management should aim to be aware of this shift and take the opportunity to revisit the fraud risks and controls. It is essential that fraud risk is reconsidered during this period of transition. If the low-friction counter-fraud measures that were appropriate during the initial response are maintained, fraudsters are likely to identify and take advantage of any unaddressed vulnerabilities.

Internal fraud

Finally, while this toolkit discusses a number of fraud risks posed by external sources, the likelihood of internal fraud has also increased significantly as a result of COVID-19.

Several factors contribute to this risk, including a perceived (or actual) relaxation of the usual integrity controls and processes due to the required speed of the emergency response and reduced oversight and scrutiny of processes due to the remote working environment. There is also an increased information security risk (covering both inadvertent disclosure and vulnerability to ‘hacking’) due to the use of new and potentially less secure IT systems and tools.

The responses to these increased risks require consideration of all the matters considered above, but in particular:

- Communicating to staff that speed of delivery cannot compromise integrity of the process and that oversight will be maintained.
- Ensuring that existing decision-making processes, delegations, controls and oversight mechanisms (particularly for high risk areas or transactions) are maintained and strictly observed.
- Keeping records (which are unable to be manipulated) which allow the circumstances of payments and/or relief delivery to be revisited and audited.

About the Serious Fraud Office

The Serious Fraud Office is the lead law enforcement agency for investigating and prosecuting serious financial crime, including bribery and corruption. Detection, investigation and prosecution of serious and complex financial crime, including corruption and bribery, is at the heart of what we do. We are also committed to preventing these crimes.

If you require further information about this toolkit, or if you would like assistance in relation to the design, implementation or operation of a specific relief programme or if you wish to report any instance of suspected fraud in the context of COVID-19 relief, then please contact the Serious Fraud Office at counterfraud@sfo.govt.nz.