

# **Independent Assessment of the Ministry of Social Development's Polices, Practices and Operations to Identify, Investigate and Prevent Fraud**

Murray D Jack  
30 August 2019

## **CONTENTS**

Executive Summary

1. Background and approach to the Assessment
2. Current state of fraud management and oversight
3. Policies, practices and operations
4. Use of intelligence
5. Assurance and quality management
6. Trends in fraud strategy and management

## **Executive Summary**

The Ministry of Social Development (MSD) commissioned this independent assessment of its approach to fraud prevention and investigations as part of its response to a review by the Office of the Privacy Commissioner ("Inquiry into the Ministry of Social Development's Exercise of Section 11 (Social Security Act, 1964) and Compliance with the Code of Conduct") released in May 2019. The Office of the Privacy Commissioner's report highlighted a number of concerns with the conduct of MSD's investigations into benefit fraud.

The purpose of the Assessment is to identify potential improvements to the policies, practices and operations of MSD's approach to the identification, investigation and prevention of external fraud.

The external fraud and investigations activity fits within a broader approach to integrity management within MSD. This incorporates the Fraud Intervention Services function, Integrity Intervention Centre, the Allegation Line and the Intelligence Unit.

Organisational changes over 2015-2017 initially saw the devolution of external fraud intervention activities from a nationally focused function to the regions. A national function was re-established in 2017 but with limited capacity at the centre.

MSD's strategy to manage the risk of external fraud has a stated focus on prevention and early intervention, which is in line with best practice. The strategy has seen investment in data matching and intelligence activities. However, the functional separation of these activities from the fraud intervention activity has reduced their effectiveness. This, combined with the devolved fraud intervention services model, has impeded the effective implementation of a best practice prevention and early intervention model.

Whilst there is recognition of external fraud risk and identification and assessment of mitigations, MSD has yet to confirm its appetite and tolerances for fraud risk, which is necessary to guide the level of investment made in mitigating fraud risk.

There are appropriate governance structures in place for oversight of fraud risk through the Risk and Audit Committee and the Organisational Integrity and Capability Governance Committee. Operational oversight is provided by the Service Delivery leadership and the national office. However, the operational oversight weakened under the devolved model, and in particular the reduction in resources and capability at the national level.

At an operational level most of the expected policies, procedures, systems and quality frameworks are in place. However, there has been little recent investment in updating and enhancing them, and there is regional variability in compliance. As noted in the Privacy Commissioner's report there is a particular need to update those related to the use of MSD's information gathering powers.

There is a comprehensive training programme for new investigators. Importantly this covers the full life-cycle of fraud investigations, including the obligations arising from statutes, case law, public sector and MSD policies. However, the training materials have not been updated over time and will require enhancement to address the recommendations in the Privacy Commissioner's report. There is less investment in on-going training and development for experienced investigators.

A Decision Support Tool (DST) is used to assist in the streaming and management of work flow.

Enforcement actions are governed by the Solicitor-General’s Enforcement Guidelines. The recent establishment of the Prosecutions Review Panel is aimed at driving more consistency in decision-making, although there is some risk this will be at the expense of efficiency.

The following table assesses the extent to which there are existing elements in place in each of the process/activity domains. This makes no assessment as to whether these are fully implemented or complied with. Additionally there is an assessment as to the extent what is in place represents best practice on a 0-5 scale, where 5 represents best practice.

<b>Domain</b>	<b>In place</b>	<b>Best practice</b>
MSD Fraud Strategy	Yes	3
Risk Appetite	Yes	1
MSD Governance	Yes	4
Operational Oversight	Yes	1
Policies and procedures	Yes	3
Systems	Yes	3
Enforcement Strategy	Yes	3
Training	Yes	3
Quality Management Systems	Yes	3

Overall, the picture is one where there are a number of elements in place, but where investment is required if they are to be lifted to best practice. The recommendations focus on specific initiatives that, if implemented, will result in best practice mitigation of the risk of external fraud.

### **Recommendations**

1. Using the existing enterprise risk framework, confirm MSD’s risk appetite and tolerance levels for external fraud. This will necessarily require work to quantify the potential level of fraud and the engage with the Government on levels of tolerance. This work should differentiate between levels of fraud, for example involvement of organised crime, exploitation of vulnerable clients, deliberate material fraud, minor fraud, and inadvertent breach. The risk appetite and tolerances should cascade down through the Service Delivery and fraud management functions. The result of the risk appetite work will ultimately determine the level of investment to be made in mitigating and managing fraud risk.
2. Form a single External Integrity function within Service Delivery. This should include the current Fraud Intervention Services, Intelligence Unit, data matching and allegation line functions. It should be headed by the Tier 3 manager reporting the DCE Service Delivery and be part of the Service Delivery Leadership Team. The national office should be sufficiently resourced to effectively provide direction, ensure there are appropriate and regularly reviewed policies and procedures, ensure external fraud operations are supported by fit-for-purpose systems and training, and provide operational oversight and reporting. Regional teams should continue to be located at the regional offices and report to the head of the External Integrity function.
3. Consider establishing a small enterprise-wide data analytics capability, separate from Service Delivery and the External Integrity Function, to conduct meta data analysis to assist in sizing the potential extent of external fraud and help focus external fraud

risk management strategy. This will also enable some oversight of the effectiveness of the External Integrity function.

4. Develop an integrated framework for external integrity that encompasses all the elements of the fraud risk management operating model under a prevent, detect, respond, and report and evaluate model. The operating model will include the necessary processes, policies, procedures, protocols, systems and methods. Many of the elements for this already exist in part but there is a need to update and enhance them to ensure they align with MSD's risk appetite and strategy.
5. Develop a revised prioritisation process that is linked to MSD's risk appetite and tolerance for external fraud and its strategy for fraud management. Support the new process with appropriate systems and tools, training, use of intelligence and operational oversight.
6. Ensure that fraud risk is built as a specific thread into service design (in a similar way to privacy and security) and that external integrity capability is included in service design governance. Service design outcomes should ensure the control environment remains aligned to MSD's risk tolerances for fraud.
7. Position the External Integrity function as a service provider to Service Delivery and take advantage of opportunities to:
  - a. Build close advisory relationships with frontline staff and consider training and tools that can be deployed in support.
  - b. Add capabilities with skill sets that are better aligned to an early intervention strategy.
  - c. Ensure the External Integrity function drives training requirements.
  - d. Utilise best practices and experiences from peer organisations in New Zealand and internationally.
8. Further develop intelligence and detection capabilities:
  - a. Hiring more data science and analytics skills.
  - b. Considering the use of artificial intelligence and machine learning technologies in core processing systems.
  - c. Consider using behavioural economics approaches in service and controls design.
9. Review investigation approaches to consider:
  - a. More flexible resource allocation through use of virtual teams and cross region working.
  - b. Shifting focus further from hard evidence gathering to facilitation and self-modification.
10. Invest in investigation skills and capabilities:
  - a. Building on the induction training programme enhance content and delivery to ensure training aligns to the needs of a prevention and early intervention strategy.
  - b. Put in place a development programme to provide on-going learning and capability building.

# **1. Background and approach to the Review**

## **Background**

The Ministry of Social Development (MSD) commissioned this independent assessment of its approach to fraud prevention and investigations as part of its response to a review by the Privacy Commissioner ("Inquiry into the Ministry of Social Development's Exercise of Section 11 (Social Security Act, 1964) and Compliance with the Code of Conduct") released in May 2019. This Inquiry raised serious concerns about some of the approaches MSD had taken to the use of its powers to investigate and pursue benefit fraud.

The purpose of the Assessment is to identify potential improvements to the policies, practices and operations of MSD's approach to the identification, investigation and prevention of fraud.

## **Scope of the Assessment**

The focus of the Assessment is on the activities and operations that relate to the approach to external fraud. These are principally, but not entirely, conducted within the Fraud and Investigation function.

Out of scope are any activities or operations related to internal fraud.

The focus is also forward-looking, seeking to identify improvements that can be made to ensure compliance with the law and best practice. The Assessment does not examine the Privacy Commissioner's review and recommendations and does not examine individual cases, historic or current, of fraud or potential fraud.

The terms of reference for the Assessment is included in Appendix A.

## **Approach to the Assessment**

The approach was to identify the elements of best practice and to assess the policies, practices and operations against them.

The Assessment sought and received a significant amount of information on current policies, practices and operations. Interviews were conducted with MSD management and staff within the fraud and investigations function and other parts of MSD as required. Discussions were also held with other organisations, in New Zealand and internationally, that have similar fraud and investigations responsibilities.

## **2. Current state of fraud management**

### **Context**

The external fraud and investigations activity fits within a broader approach to integrity management within MSD. This incorporates the Fraud Intervention Services function, Integrity Intervention Centre, the Allegation Line and the Intelligence Unit.

Prior to a restructure in 2015 the Fraud Intervention Services function was a national unit, with operations located in MSD's regional offices. As part of the restructure the national management of fraud teams unit was devolved to the 11 regional offices and the fraud and investigation activities reported to the relevant Regional Commissioners. A small national team remained to provide strategic direction, reporting, support and coordination.

In September 2017 reporting lines were shifted from the Regional Commissioners to a re-established National Manager Fraud Intervention Services role, reporting to a General Manager Integrity and Debt. At the same time the national office team was dis-established with the intent that its functions would be carried out by other parts of Service Delivery. This did not occur as most of the capability of that team left the organisation. The National Manager had limited support resources.

Over the past few years MSD has had a strategy to shift the focus of effort from response through investigations and prosecutions to prevention and early intervention. This has resulted in reductions in prosecutions. It is noted that, as is common, a change of government in 2017 has brought a change in focus and approach to administration of welfare benefits that also affects the approach to fraud strategy.

Many of the benefits MSD administers are targeted at some of New Zealand's most vulnerable people. The rules applying to entitlement, both initial and on-going, are often complex creating opportunities for inadvertent compliance breaches.

It is also the case that there is scope for and evidence of significant deliberate fraud.

### **Current Structure**

The Fraud Intervention Services national management activity sits within the Client Service Support function of Service Delivery and is led by the General Manager Integrity and Debt, a Tier 4 role. Operations are managed by a National Manager Fraud Services with the regional teams embedded within Service Delivery Regions. Fraud Intervention Services plans and conducts investigations at the regional level. There are approximately 160 people within the Fraud Intervention function. It is noted that the national function comprises four people and as designed is able to offer only limited operational support to the intervention services teams in the regions.

Training of investigators is provided by a training organisation under the National Manager, Training and Quality, who reports to the General Manager, Client Service Quality.

Fraud investigators are supported by the MSD Legal Services team, primarily when investigations become enforcement actions.

The data intelligence activities are part of the Risk and Audit function that sits within Corporate Solutions. It is noted that an Integrity Coordination Group that seeks to mitigate

the risks associated with a lack of coordination across the integrity activities in MSD has been established.

## **Fraud strategy**

In 2015/16, recognising that debt owed by clients and former clients was growing (at that time \$1.32 billion), with debt recovery not keeping pace with debt creation, Service Delivery developed a strategy approach and action plan based on prevention and early intervention. This strategy acknowledged MSD's Simplification Project (a programme that looks to streamline service delivery practices and processes using digital and technology solutions) provided an opportunity to improve client service but also a challenge to a fraud prevention strategy unless fraud prevention measures were designed into the new processes, policies and systems. Removing some control processes to improve efficiency through, for example self-service, has increased the opportunity for fraud.

The strategy noted the focus on prevention would require a strong focus on soft skills and staff behaviours for frontline staff in order to integrate fraud prevention into client case management practices.

At the time this strategy and action plan was being implemented Service Delivery undertook the 2017 restructure. The devolution of fraud intervention services and the retention of limited central support has impeded progress. In February 2019 there was a renewed commitment to the prevention and early intervention model.

Key to a prevention strategy is effective use of data for intelligence and prioritisation.

## **Risk appetite**

The risk posed by external fraud is recognised as a Ministry-wide risk. It has an inherent and residual rating of "high". Several controls are identified; the client debt management strategy, allegation line, online inter-agency information sharing, Social Sector Accreditation Standards, and independent assessments and reviews. These are assessed as "functional" with the exception of the debt strategy which is assessed as "defined".

The risk appetite at the MSD-wide level has been identified at a high level but needs further elaboration. Risk tolerances have not been set.

Whilst there is data on the extent of external fraud detected and recoveries made (or established as debt) there is no estimation of the potential extent of fraud.

## **Oversight**

The Fraud Intervention function reports through the Client Service Support function to the Service Delivery executive leadership team.

At the MSD-wide level oversight is provided through the Organisational Integrity and Capability Governance Committee. Discussions relating to external fraud occur periodically. In addition the Risk and Audit Committee also receives periodic updates on external fraud.

While there is some statistical reporting there is little in the way of regular operational reporting in terms of performance against key measures.

There is regular reporting to the Service Delivery leadership but there is room for improvement, some of which was identified in the Office of the Privacy Commissioner's report.

### **3. Policies, Procedures and Operations**

#### **Fraud operations**

There are a number of detailed operating policies and procedures on Doogle (MSD's corporate intranet) that cover most of the fraud investigation life-cycle. These contain detailed guidance for the conduct of investigations, for example on the gathering, analysis, interview, decision and sanction phases of investigations, and processes for search warrants and prosecutions.

Whilst much of what is required is covered it is not organised as a coherent set of policies and procedures and has not been subject to regular review and update.

It was noted in the interviews that the devolution of external fraud activities resulted in some divergence from the policies and procedures as different regions developed local practices.

#### **Prioritisation**

Historically prioritisation of allegations was facilitated by the Decision Support Tool (DST) built into the Investigation Management System (IMS). The DST assigned a score for each allegation to a range of factors that were input into the IMS at the time the allegation was raised and recorded. Allegations with a score exceeding a threshold were determined to be "high risk" and these are then input into a regional work queue and allocated for investigation as workload permitted. Thresholds were reviewed periodically.

There was significant judgement applied in assessing scores (for example taking into account the availability and quality of information) and in assessing whether an allegation should be investigated as a case. As a result of this assessment, not all cases assessed as high risk continued to an investigation, but the majority did so.

It should be noted that not all cases would proceed through this process, for example if the case arose through means other than the allegation line.

Since February 2019 the DST system has been used as the principal tool for assisting in the streaming and management of work flow. Based largely on the alleged period of offending work is streamed into early intervention, facilitation or investigation. Early intervention work is assigned nationally, and facilitation and investigation cases are assigned regionally. Once streamed cases are reviewed to confirm they have been allocated to the correct stream before any investigation activity commences.

#### **Enforcement**

The enforcement approach is governed by the Solicitor-General's Prosecution Guidelines. There are detailed policies that govern decisions on matters that may be referred for prosecution.

In May 2018 a Prosecution Review Panel was established with authority to make decisions on cases considered for fraud prosecution. This initiative was aimed at improving consistency

of decisions. All cases are reviewed by MSD's legal team prior to being considered by the Panel. There are guidelines for the Panel's decision-making. The Panel's role is limited to considering the Public Interest Test, which requires among other things consideration of MSD enforcement priorities. Whilst there is some guidance on the matters to be considered there is not a clear linkage to MSD's priorities.

A service level agreement governs the relationship between MSD Legal and the Fraud Intervention function. Although it has not been reviewed since its implementation in 2004 it is believed to still reflect the nature of the relationship and services provided.

## **Code of conduct**

Section 11 of the Social Security Act 1964 (the Act) provides MSD with powers to obtain information for specified purposes. Section 11B of the Act also requires MSD to issue a Code of Conduct to govern the requirements applying to the obtaining of information. MSD issued the Code of Conduct on 12 September 2012 after consultation with the Privacy Commissioner. All officers or employees of MSD must comply with the Code. The Code governs the operation of Section 11 of the ACT and limits what information may be requested.

The Code provides for the ability to request information under Section 11 without notifying clients where there are reasonable grounds to believe that compliance with this part of the code would prejudice the prevention, detection, investigation, prosecution or punishment of an offence; or the imposition of a pecuniary penalty" (this is termed "prejudice of the maintenance of the law").

It had become the practice for investigators to often resort to use of this power, particularly for cases assessed as "high risk" by the DST.

## **Training**

There is a very extensive training programme for new investigators. This is a seven week programme and includes training on the benefits administered, benefit systems, fraud relationships, investigation modules and processes, evidence gathering, interviewing, statement taking, prosecution modules and analysis and decision-making and compliance with legislation (including the Privacy Act, Official Information Act, Acts administered by MSD) and case law.

Delivery includes facilitated sessions, eLearning, workshops, case studies and simulation.

Although comprehensive, the training materials have not been reviewed and updated for changes in policies and practices. Specific enhancements will also be required as a result of the recommendations in the Office of the Privacy Commissioner's report.

Whilst all new investigators pass through this training there is little formal on-going training and development for experienced investigators.

As has been noted previously the training is provided by teams within the Client Service Quality function. This may provide challenges in keeping the training experience current.

## **Case management**

Caseloads are managed at the regional level with little or no resource allocation across regions. The primary tools used are the DST and the IMS. The IMS covers the life-cycle including allegation, investigation, enforcement and/or sanction, and outcome. It enables individual investigation plans, case notes, instructions to technical officers, and referrals for prosecution to be recorded and tracked.

This a comprehensive system in terms of the process life-cycle but needs enhancement to build reporting and analytics capability.

Decisions on cases are made at the regional level, with prosecutions also passing through the Prosecution Review Panel. There is no process for escalation of decisions on cases to the national level.

## **4. Use of intelligence**

The Intelligence Unit has some capability and utilises a number of tools to provide intelligence on potential fraud.

Substantial use is made of MSD's Information Analysis Platform (IAP), an enterprise data warehouse that replicates MSD's core systems on a daily basis. This database provides a wealth of data from which insights can be developed. The principal mining tool is SAS Enterprise Guide.

The main presentation tools are i2 Analyst's Notebook and ArcGIS pro, the latter allowing creation and sharing of geographic information.

The tools used provide the appropriate capability to support an effective intelligence function.

MSD also makes extensive use of data matching with other government agencies. This activity is governed by data sharing agreements.

Whilst there is some analytic capability there is an opportunity to enhance it by adding more resources with data science/analytics expertise.

As has been noted the intelligence functions are located within the Risk and Assurance part of Corporate Solutions. This is not optimal. Risk and Assurance is the third line of defence so there is a potential conflict with an operational activity. Additionally the intelligence functions would benefit from a closer relationship with Fraud Intervention Services as this reduces the need for other means of coordinating activities, more readily aligns intelligence and investigation priorities, and has more direct feedback loops from frontline staff and investigators.

## **5. Assurance and quality management**

### **Assurance**

MSD has a well-developed risk and assurance function with a risk-based annual plan. Fraud investigation processes were the subject of specific review in the 2015/16 Work Programme, and Client Debt Management in 2016/17 and 2017/18.

The work of the risk and assurance function is overseen by the Risk and Audit Committee which meets periodically. The minutes of this committee indicate that there is regular oversight of the risk and assurance work programme.

### **Fraud Intervention Services quality programme**

A new Quality Assurance Framework was introduced in 2017 and was designed to provide assurance on the quality of investigations, encourage best practice, and provide feedback to staff. The framework sets minimum standards for investigations and a monitoring process based on the experience of the investigator. Investigations are carried out by Fraud Intervention Services Managers, or their delegates.

Separate Quality Assessment Reports are prepared for Investigations, Facilitation and Technical Officers (IMS Case quality and Benefit Processing Quality). The scope of the Investigations review includes compliance with applicable legislation, case law, MSD policy, and Solicitor-General Guidelines. Reports are submitted to the National Fraud Intervention Services office.

This comprehensive process is intended over time to cover all investigators and technical officers. However, with the devolution of investigations to the regions there was some variability in the application of the framework. The lack of resources has constrained effective oversight of this process.

## **6. Trends in fraud strategy and management**

There are three principal trends in the approaches to managing fraud risk in organisations with profiles similar to that of MSD.

### **A focus on prevention**

There is a well-recognised move away from a sole focus on reactive responses. MSD has recognised this trend with its stated strategy of prevention and early intervention.

An effective prevention and early intervention strategy depends on a strong control environment (procedures, practices and systems) that minimises the opportunity of fraud occurring. Also required is a shift in culture for both frontline staff and investigators supported by training and development and some new skills and capabilities.

Despite a pivot to prevention, there is still a need for effective response once significant fraud is identified. This requires the right skills and capabilities to be able to facilitate optimal outcomes. Effective response provides an important deterrent effect.

### **A focus on data and intelligence**

Organisations are investing in both skills and tools to materially lift capabilities to analyse data and develop insights to assist in fraud detection, prioritise resourcing of investigations and provide feedback loops to continuously improve approaches and practices. These initiatives extend to the embedding artificial intelligence and machine learning techniques into core operational systems to be able to detect fraud at source.

MSD has made investments in intelligence and data matching capabilities but opportunities remain to extend these and better integrate them with fraud intervention services.

### **Building an enterprise approach**

The move to prevention and use of intelligence is driving stronger cross-enterprise approaches to fraud risk management. Control environment improvements require fraud risk management to be a thread that runs through service design (process, systems and people), in the same way that privacy and security are now commonly seen as integral to service design.

A balanced prevention and response strategy requires assembly of a broad set of capabilities that need to collaborate effectively to result in effective risk management of fraud.

## **Appendix A**

### **Independent Assessment of the Ministry of Social Development's Polices, Practices and Operations to identify, investigate and prevent fraud**

**5 April 2019**

The Chief Executive of the Ministry of Social Development (the Chief Executive) has commissioned an independent assessment of the Ministry of Social Development's (the Ministry) policies, practices and operations to identify, investigate and prevent fraud (the Assessment).

The Assessment will be carried out by Murray Jack ("the Assessor") on behalf of the Chief Executive.

#### **Objectives of the Assessment**

The objective of the Assessment is to:

- identify the current polices, practices and operations to identify, investigate and prevent fraud,
- assess those polices, practices and operations having regard to relevant Law, good practice;
- assess the current plans for enhancement of fraud practices; and
- provide recommendations for any improvements.

#### **Matters in scope**

The Assessment will consider the Ministry's policies, practices and operations used to identify, investigate and prevent allegations of external<sup>1</sup> fraud.

The Assessment will consider how the Ministry:

- obtains and manages fraud related intelligence
- manages and assesses/evaluates allegations of fraud
- investigates cases of alleged fraud including the collection and management of evidence
- determines the appropriate outcome for the cases
- ensures fairness to all participants in the investigation, including those people who are subject to the investigations.

In particular the Assessment will consider whether the Ministry has an appropriate operating model in the relevant area including, but not limited to:

- the necessary people and systems capability
- the appropriate operational policies in place
- assurance systems to ensure compliance with policy, practices and legislation

The Assessment will take into consideration the Legislative and Policy settings under which the Ministry progresses fraud investigations.

It will also take into consideration current plans for enhancement of fraud practices including the proposed prevention approach.

---

<sup>1</sup> These are allegations of fraud relating to the Ministry's clients or external parties, not allegations relating to the Ministry's own staff.

## **Matters out of scope**

The Assessment will not consider processing internal fraud investigations except where policies and processes intersect with external fraud.

## **Additional Expertise**

The Assessor may, with the approval of the Chief Executive, may engage additional specialists to support the Assessment. This can include, but is not limited to, legal, forensic and privacy expertise.

## **Deliverables and timeframes**

The Assessor will deliver a report for the Chief Executive in accordance with the following timeline:

5 April 2019	Terms of Assessment approved and Assessment commences
28 June 2019	Draft Report and Recommendations
9 August 2019	Final Report and Recommendations Completed

## **Amendment**

Amendments to the terms of reference, including the timeframes or the sequencing of reports, may be made with the written approval of the Chief Executive.

## **Support**

MSD shall provide the Assessor with:

- Secretariat services for the Assessment
- Office space at MSD premises
- Administrative support
- Access to all documentation and material related to matters in scope of the Assessment
- Access to staff for interviews
- Fund and support the Assessor in engaging any additional specialist

Secretariat services for the Assessment will be provided by the General Manager Risk and Assurance.

## **Governance**

The Assessment will be supported by the Deputy Chief Executive, Corporate Solutions.

The Assessor will have direct access to the Chief Executive during the Assessment.

Approved this 5<sup>th</sup> day of April 2019.

Debbie Power  
Chief Executive  
Ministry of Social Development

