SFO
SERIOUS FRAUD OFFICE
TE TARI HARA TĀWARE

Counter Fraud Centre
TAUĀRAI HARA TĀWARE

CASE STUDY – SEPTEMBER 2026

Fraudulent company incorporations used to abuse government support schemes

The Counter Fraud Centre – Tauārai Hara Tāware is the prevention arm of the Serious Fraud Office, leading counter fraud efforts in New Zealand's public sector. Using actual cases prosecuted by the Serious Fraud Office, our case studies aim to help public organisations understand, identify and prevent the impact of fraud.

Why are case studies useful?

Use case studies to:

- **increase fraud awareness** by including them in online training modules or team discussions
- **identify fraud risks** by considering whether the circumstances in this scenario might happen at your organisation
- **prevent fraud** by considering the controls that could prevent this fraud from occurring and implementing similar measures in your organisation.

What is in this case study?

- Case information
- Prosecution outcome
- Impact of offending
- Fraudster personas
- Red flags
- Effective controls
- Strengthening counter fraud capability

Case information

Individual used stolen identities, forged company records, false tax returns and fraudulent funding applications to steal more than $600,000.

Background

Deceptive collection of identification and company formation

An individual obtained personal information, such as identification documents and IRD numbers, about several individuals through fraudulent means. This was done by placing false advertisements for work and misleading individuals applying for tenancies into providing their personal details. The affected individuals were unaware that their identities would later be used to commit fraud.

The individual used this information to incorporate multiple companies through the New Zealand Companies Office, submitting 16 forged director and shareholder consent forms in relation to nine New Zealand companies.

These illegitimate companies were subsequently used to file false goods and services tax (GST) returns and apply for COVID-19 subsidies to which they were not entitled.

Goods and services tax fraud

Using these companies, the individual submitted false GST returns to Inland Revenue. He filed 58 GST returns, of which 13 were paid, resulting in $22,010.27 obtained from $272,090.79 claimed.

In some instances, GST returns were filed for shell companies that either had no bank accounts in New Zealand, had no transactions during the relevant period or had only bank fee activity. In other cases, the individual created the appearance of legitimate business transactions by transferring funds between the company accounts, thereby creating the false impression of revenue and expenses where none existed.

COVID-19 wage subsidy fraud

From 2020, the Government implemented the wage subsidy scheme to support businesses affected by COVID-19 to retain employees and provide them with an income when they were unable to work. Operating in a high-trust environment, the scheme enabled rapid access to funding and relied on applicants' self-declarations of eligibility.

The individual submitted 42 wage subsidy scheme applications to the Ministry of Social Development, totalling $1,371,986, using fake companies he had incorporated to receive support. Of the 42 applications submitted, 29 were declined and 13 were approved, resulting in payments totalling $602,202.40.

Inland Revenue COVID-19 subsidies

Inland Revenue also administered additional COVID-19-related subsidies, including:

- Small Business Cashflow Loan Scheme: designed to support small-to-medium businesses experiencing a loss of revenue due to COVID-19.
- Resurgence Support Payment: provided assistance to viable, ongoing businesses that experienced at least a 30% decline in revenue due to an increase in COVID-19 alert levels.
- COVID-19 Support Payment: aimed at supporting viable, ongoing businesses that experienced a 40% reduction in revenue as a result of specific COVID-19 circumstances.

The individual submitted 10 applications across these schemes, totalling $172,800. None of these applications were successful.

Beyond opportunistic fraud

The court found that the offending extended beyond opportunistic conduct during the COVID-19 period. Instead, it formed part of a broader pattern of deliberate and premeditated behaviour, characterised by persistent and repeated acts of dishonesty over time. The offending also involved multiple agencies, which limited end-to-end visibility of the offending and reduced the likelihood of the full fraud pattern being identified early.

For more information about this case see sfo.govt.nz/media-cases/cases/hun-min-im.

Prosecution outcome

The individual pleaded guilty to 54 charges of dishonestly using a document and was found guilty following trial on a further 18 charges of obtaining by deception and 16 charges of using a forged document. He was sentenced to 4 years and 4.5 months imprisonment.

Impact of offending

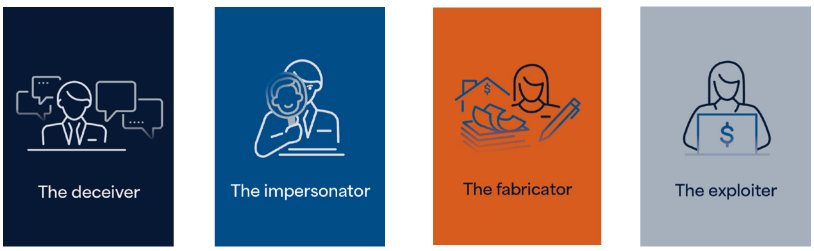
- Over $624,000 in public funds was fraudulently obtained, diverting resources intended to support businesses and workers during a national emergency.
- Exploiting emergency support schemes risked reducing confidence in government programmes and may have affected timely support to legitimate recipients.
- The impact could have been far more severe were it not for control systems in place at Inland Revenue and the Ministry of Social Development, which prevented an additional $1.2 million worth of applications being accepted.

Find out more about the impacts of public sector fraud at sfo.govt.nz/counter-fraud/guidance/impacts-of-public-sector-fraud.

Fraudster personas

In this case there were four main personas.

- **The deceiver** – the individual misled others through fake job advertisements, deceptive tenancy interactions and false appearance of legitimate business activity, enabling him to obtain personal information and access funds dishonestly.
- **The impersonator** – the individual used fraudulently obtained personal information to falsely present himself as others to establish companies and submit fraudulent applications.
- **The fabricator** – the individual submitted 16 forged director and shareholder consent forms, filed false GST returns and created artificial financial activity to support fraudulent claims.
- **The exploiter** – the individual took advantage of high-trust systems and self-declaration processes by using fake companies he had established to access support schemes for financial gain.



Find out more about fraudster personas at sfo.govt.nz/counter-fraud/guidance/fraudster-personas.

Red flags

While red flags do not necessarily indicate fraud, they can be a sign that something is out of the ordinary and may need to be looked into.

- **Use of multiple newly incorporated entities** – the individual created multiple newly incorporated companies linked to common identity information. These entities appeared to be legitimate businesses but were in fact used to facilitate fraudulent activity.
- **GST filings inconsistent with genuine operations** – GST filings across these entities were not consistent with normal business activity, indicating that the reported transactions were fabricated or did not reflect genuine economic activity.
- **Concentrated volume of funding applications across linked companies** – a high volume of funding applications was submitted across related companies, indicating coordinated activity rather than independent business claims.
- **Persistent and iterative application behaviour** – the individual continued to submit further applications despite previous unsuccessful attempts, demonstrating a deliberate and sustained effort to obtain funds through fraudulent means.

Effective controls

These are examples of controls that could have been helpful in this instance.

- **Approval workflow** – ensure applications are appropriately reviewed and approved to reduce the risk of fraudulent payments.
- **Automated data matching and monitoring** – monitor and match data and information to identify inconsistencies, duplicate claims or linked entities.
- **Coordinated disruption activity** – coordinate disruption activities across multiple programmes or agencies to strengthen processes for identifying serious or organised criminals.
- **Eligibility requirements** – define and apply clear criteria that must be met before a claim or application is approved, limiting access to support to only those who meet the requirements.
- **Exception reporting** – generate reports to identify unusual activity, such as a high volume of applications or irregular payment patterns that may require further review.
- **Fraud investigation processes** – investigate suspected fraud in line with defined policies and report to related authorities.
- **Identity verification** – authenticate client or third-party identities by verifying identity information and credentials to ensure the person or entity is who they claim to be.

Find out more about effective fraud countermeasures at sfo.govt.nz/counter-fraud/guidance/fraud-controls.

Strengthening counter fraud capability

Application and approval controls

- Are high-risk applications subject to appropriate review rather than automatic approval?
- Are there controls in place to verify business legitimacy before payments are made?
- Are application processes designed to identify inconsistencies in submitted information?

Monitoring and review

- Is the organisation able to identify patterns across multiple entities or related applications?
- Are repeated or unsuccessful applications identified or flagged for further review?
- Is there oversight of high-volume or unusual claims activity?

Information sharing and coordination

- Is information shared effectively across teams or agencies to identify linked fraud risks?
- Are emerging risks analysed and acted on in a timely manner?

Capability and awareness

- Do employees understand fraud risks and how to identify and report suspicious activity?
- Is there an appropriate balance between rapid service delivery and effective fraud risk management?

Find out more about free online tools your organisation can use to strengthen its fraud and corruption controls at sfo.govt.nz/counter-fraud/tools.

Need help?

Wherever you are with your counter fraud efforts, we're here to help.

The Counter Fraud Centre offers a range of resources to help build capability across your organisation. If you are in the public sector and would like to contact us about the services we can provide, please email counterfraud@sfo.govt.nz or visit sfo.govt.nz/counter-fraud/counter-fraud-centre.