SFO
SERIOUS FRAUD OFFICE
TE TARI HARA TĀWARE

Counter Fraud Centre
TAUĀRAI HARA TĀWARE

CASE STUDY – MARCH 2026

Employee exploits weaknesses to steal over $1 million in trust funds

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 countermeasures that could prevent this fraud from occurring and implementing similar controls in your organisation.

What is in this case study?

Case information

An employee with access to financial systems created fraudulent transactions, altered invoices and fabricated a contract to conceal the fraud.

Te Roopu Awhina Ki Porirua Trust (**the trust**) was established to provide welfare, health and education services to whānau and tamariki in Porirua.

In 2020, the trust's annual revenue increased significantly to $10.6 million, largely due to the $6.3 million in funding from Oranga Tamariki to provide care services for at-risk children. By 2021, the trust's annual revenue had further increased to $14 million.

An employee began working for the trust as a part-time financial administrator in June 2019 and moved to full-time in October 2019. Her responsibilities quickly expanded from managing payroll to further responsibilities including finance. This gave her access to the trust's accounting system, payroll platform and online banking system.

Over a period of about six months, the employee stole more than $1 million of trust funds. She exploited weaknesses in payment authorisation and account controls by:

1. Creating 79 fraudulent transactions worth $772,000 by substituting her bank account details for those of genuine suppliers. These payments required two authorisations. The employee completed the first herself and obtained the second from senior staff - initially using altered invoices, later without any supporting documentation.
2. Making 185 unauthorised transfers totalling $291,766 from accounts that did not require dual authorisation. She concealed the transactions by using genuine supplier names in the payee field.
3. She also used the trust's debit cards to pay directly for online gambling services.

Exploited weak accounting system processes

All the trust's bank accounts were linked directly to accounting software that generated an unreconciled entry for every payment. Each entry required reconciliation, including assigning a customer or supplier, selecting an accounting code or cost centre and recording the user who reconciled it.

The employee exploited this process by reconciling 353 fraudulent payments totalling $827,806:

- 231 payments to her account ($790,031)
- 122 payments to gambling sites ($37,775).

To conceal the fraud, she coded these transactions as legitimate expenses. For example:

- A payment of $8,915 that she made to herself, was coded to the supplier Spark as telephone, tolls and internet expenses.
- Gambling transactions were disguised as motor vehicle expenses. Payments to gambling site BP Group Malta Ltd were coded to BP.
- Payments to other gambling sites were coded to Microsoft and accounted for as subscriptions.

Created false contract and invoices

When the employee's bank raised concerns about the regular, large deposits from the trust to her personal account and threatened to freeze or close her accounts, the employee created a cover story. Using the trust's official accounts email address, the employee impersonated a former accounts person and claimed that she was contracted to the trust for management services and held an executive role with the trust.

She attached:

- a fabricated contract for services agreement between her and the trust
- 15 false invoices in her name, matching the amounts of the misappropriated funds deposited into her account.

For more information about this case see sfo.govt.nz/media-cases/media-releases/former-charity-worker-sentenced-to-3-5-years-imprisonment-in-sfo-case.

Prosecution outcome

- The employee pleaded guilty to one representative charge of obtaining by deception and one charge of failing to appear. She was sentenced to three and a half years' imprisonment.

Impact of offending

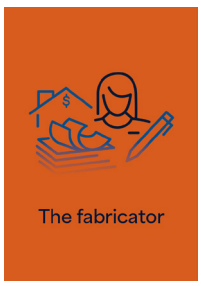
- The trust lost over $1 million and the scale of the fraud threatened its ongoing existence.
- Funding was placed at risk; the trust only secured further funding after an iwi intervened and committed to a stronger management regime.
- Employees experienced significant personal shame, fearing the community would associate them with the fraud.
- Vulnerable members of the community lost out on the support the trust could have provided had the funds not been stolen.

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 fabricator** – the employee created false supplier invoices to get the payments to her account authorised. She also fabricated an employment contract and created false invoices to justify the deposits.
- **The deceiver** – the employee deceived her bank, claiming she had a legitimate contract with the trust. She also misled the bank into believing she held an executive position at the trust.
- **The impersonator** – the employee impersonated a former employee when corresponding with the bank.
- **The exploiter** – the employee took advantage of weak payment authorisation processes and lack of oversight in reconciliations.



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.

- **Addiction, like gambling or substance abuse, can create financial pressure** – the employee used debit cards related to the offending to pay for online gambling and would code some gambling expenses as if they were legitimate trust expenses.
- **Unwillingness to share duties or delegate financial responsibilities** – the employee was the primary access point for all the trust's financial systems
- **Sole signatory on bank accounts or lack of segregation of duties** – a second person, who was required to authorise payments did not check bank account numbers, only confirming the amount. An additional $291,766 was transferred directly from the trust's accounts to the employees, without the need for a second signature.
- **Delays in reconciling accounts or providing documentation** – management would sign off payments without requiring or sighting invoices.

Effective countermeasures

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

- **Fraud awareness training** – employees should be trained and supported to identify red flags to help identify fraudulent behaviour and know what to do and how to report any suspected fraud.
- **Procedural instructions or guidance** – provide to employees clear, documented processes and guidance related to activities or processes.
- **Internal audits or reviews** – these are an objective review and assessment of the effectiveness of internal controls and risk management. Regular internal audits can increase the fear of the fraud being exposed, which can serve as a deterrent to committing fraud.
- **Segregation of duties** – distribute business process tasks among multiple staff. This prevents an employee from being able to commit and hide a fraudulent transaction.
- **Governance and oversight** – establish governance and oversight to oversee critical decisions and risks.

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

Strengthening counter fraud capability

Payment controls

- Are all payments subject to dual or multiple authorisations?
- Is there segregation of duties among those who initiate, approve, and reconcile transactions?
- Do authorisers understand their responsibility to check supporting documents before approving transactions ?
- Is there a robust process when requests are made to change vendor bank accounts in the system?

Monitoring and review

- Does your organisation regularly review financial processes to identify control weaknesses?
- Are recommendations from audits or reviews implemented promptly?
- Is there independent oversight of reconciliations and high-risk transactions?

Staff awareness

- Are employees trained to recognise red flags and suspicious behaviour?
- Do staff know how to report concerns safely and confidentially?

Find out more about free online tools your organisation can use to strengthen its fraud and corruption countermeasures 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.