Case Study

Internal audit revealed $1.2 million fraud committed against the Waitangi Trust

Background

$1.2 million fraud that impacted a whole community

An internal Corporate Services Manager responsible for all financial administration defrauded the Waitangi National Trust of $1.2 million over 15 months.

Waitangi National Trust manages the day-to-day operations of 506 hectares of historical land known as the Treaty Grounds. Whare Tiriti (the Treaty House) where Te Tiriti o Waitangi was signed, is located within the Treaty Grounds, making them a place of significant historical importance for New Zealand.

The Trust generates revenue by providing cultural experiences and historical tours, and operating a local resort. The purpose of revenue generated by the Trust is to manage and improve the Trust's property.

The employee's role was to manage all of the Trust's finances to ensure funds were being spent within the parameters of the Trust's purpose. His role included raising online transaction orders to pay vendors from the Trust's accounts.

Vulnerabilities in the Administration of Banking Systems Enabled the Fraud

The employee defrauded the Trust by exploiting weaknesses in the Trust's online banking processes. The banking system had a two-part authorisation system - one person raised the transaction order and another approved it. Once approved by the second person, the funds left the account. The employee's banking credentials allowed him to raise a transaction order, but he required the credentials of another to authorise the payment.

After obtaining the banking credentials of a former employee, he used these to authorise 43 online payments to accounts controlled by him.

He also created fake invoices to make it appear as if money was owed to legitimate vendors of the Trust. This was done to ensure large payments were reconciled and approved by the

accounts team. The invoices were processed by the accounts team with the funds being paid to accounts controlled by the employee.

The fraud was detected when the organisation employed a new manager

A new accounts manager employed by the organisation conducted a reconciliation of the accounts and found several discrepancies. The organisation engaged a consultant who, upon further investigation, found and identified discrepancies between the management accounts and audited financial statements.

The matter was referred to the Serious Fraud Office and the employee was subsequently sentenced to three years and eight months in prison.

Fraud Prevention Observations

Impacts	▶ The Trust, which is responsible for maintaining one of the most historically important places in New Zealand, was in danger of insolvency. ▶ Seasonal employees lost their jobs as there was not enough money to keep them employed. This put more pressure on full-time employees and ultimately led to the resignation of many well-trained and qualified employees due to stress. ▶ Hapori whānui (the wider community) were affected by anxiety as a result of being associated with the fraud.
Fraudster Personas	▶ **The Impersonator** – The employee obtained the banking credentials of other employees to authorise transactions. ▶ **The Fabricator** - He created false invoices to make it appear as if the funds were transferred to legitimate vendors. ▶ **The Exploiter** – He was in a position of high trust and low oversight and used his knowledge of the financial systems for his own personal gain.

Case Study

Red Flags	▶ Employees who appear to be living beyond their means - the employee was living a lavish lifestyle well beyond the expectation of someone in his pay bracket. ▶ Former employees' credentials appearing in recent audit logs - the banking login credentials of a former employee were used to authorise transactions. ▶ Employees' credentials used outside their working hours - the credentials of an employee who was on sick leave were used to login to the accounting systems.
Effective Countermeasures	This case illustrates the need for **segregation of duties** to distribute the responsibility for high-fraud-risk tasks. **Access controls** can be used to limit access to banking login credentials, and to remove credentials of former employees. **Audit** and reconciliation processes can support organisations to detect fraud in the early stages.
Mitigations and Responses	The Trust identified vulnerabilities within its internal controls. As a result, a larger finance team was employed to introduce segregated duties and role sharing.
Link to sources	SFO Media Release
Fraud Tags	Not for Profit, Administrative and Support Services, Organisation Strategy and Performance, Finance, Abuse of Position of Trust.