Case Study

$1 million fraud committed against the Christchurch District Health Board

Background

Six-year fraud used to support a lavish lifestyle

An internal eligibility specialist at Christchurch Hospital defrauded it of $1 million over a six-year period. The employee was responsible for invoicing and collecting revenue for patients who were ineligible to receive free healthcare.

The employee manipulated the Hospital's processing system and redirected 475 payments from ineligible patients to accounts she controlled. She did this by:

- offering ineligible patients unauthorised discounts for using cash which she then took for herself
- creating fake invoices with her bank details on them
- entering incorrect patient information into the Hospital's system to make it appear as if the patient met the eligibility criteria.

In an attempt to avoid detection, she used a manual accounting system to remove the debt against patients' accounts. The system did not record changes that had been made which made it appear as if the debt never existed.

The proceeds of the fraud were used to fund her lavish lifestyle and gambling addiction.

The fraud was detected following a patient query

The fraud was detected when a patient contacted the hospital to query an invoice for medical treatment that they had already paid several months earlier. Upon enquiry, the Hospital identified that the bank account on the document provided to the patient was not the Hospital's account. Further enquiries identified additional emails from the employee to patients, requesting direct payment to non-Hospital bank accounts.

Case Study

With the support of a consultant, an internal audit was carried out. It found that the employee had been asking ineligible patients to make payments to accounts controlled by her. The matter was referred to the Serious Fraud Office for investigation and the employee was prosecuted and subsequently sentenced to three years imprisonment.

Fraud Prevention Observations	
Impacts	▶ Financial loss of over $1 million to the Hospital. This money could have covered the salary of 18 graduate nurses. ▶ Multiple Hospital employees experienced considerable stress and anxiety. ▶ The misuse of private information regarding sensitive medical procedures was used to target vulnerable patients who had little knowledge and understanding of what they were required to pay for their medical treatment.
Fraudster Personas	▶ **The Exploiter –** the employee identified and exploited vulnerabilities in the Hospital's accounting and payment systems. ▶ **The Fabricator –** the employee changed the bank account on official Hospital documentation to redirect patients' payments to an account she controlled.
Red Flags	▶ Employees who don't take leave - the employee went to the office on days she wasn't working or when she was on leave. ▶ Resistance in sharing roles and duties- she insisted she was the only one that should work with certain patients. ▶ Processes that are not followed – she contacted patients outside of work hours via social media platforms. ▶ Low oversight - she had sole control over the process with little oversight.

Effective Countermeasures	This case illustrates the need for access controls to protect data from manipulation. **Automatic IT systems**, such as **audit logs**, can prevent data from being manipulated, and **parameters and limitation** controls can prevent unauthorised people from changing documents. Other effective countermeasures include **pressure testing** existing controls and **segregation of duties** to ensure that more than one person is responsible for completing high fraud risk tasks.
Mitigations and Responses	▶ The organisation engaged a consultant who identified weaknesses in the Hospital's internal controls and helped to develop a new control framework. ▶ The payment processes were reviewed and the organisation stopped accepting cash payments. ▶ Internal fraud awareness was communicated across the organisation. This included information about who to contact if fraud was suspected.
Link to sources	▶ SFO Media Release
Fraud Tags	Public Sector, Local Government, Administrative and Supportive services, Service Delivery and Operations, Finance.