COUNTER FRAUD CENTRE
Tauārai Hara Tāware

Guide to Fraudster Personas

APRIL 2023

Fraudster Personas

Through our work in investigations and prosecutions, and with our international counterparts, we have identified common tried and tested methods fraudsters use to commit financial crimes.

These personas can help you and your organisation to think like a fraudster. They can help you more easily understand the different actions fraudsters use to target government programmes and functions.

Fraudsters often use a variety of methods from several different personas. For example, they may deceive a public official, impersonate another individual, fabricate evidence, and then conceal their activity.

Knowing what these common methods are can help you anticipate how fraudsters might target a government programme or function.

The Impersonator	The Impersonator pretends they are another person or entity to dishonestly gain a benefit for themselves or another person.
The Corruptor	The Corruptor abuses their position of entrusted power to gain a benefit for themselves or another person.
The Deceiver	The Deceiver makes others believe something that is not true to dishonestly gain a benefit for themselves or another person.
The Enabler	The Enabler knowingly or complacently enables fraudulent activity to dishonestly gain a benefit for themselves or another person.
The Exploiter	The Exploiter uses something for a wrongful purpose to dishonestly gain a benefit for themselves or another person.
The Fabricator	The Fabricator invents or produces documents that are false to dishonestly gain a benefit for themselves or another person.
The Organised	The Organised are a group or people who use a combination of sophisticated methods, in a planned and coordinated way, to dishonestly gain a benefit for themselves.

The Impersonator

- ✓ The Impersonator pretends they are another person or entity to dishonestly gain a benefit for themselves or another person.
- ✓ This might involve using false or stolen identities, attributes, or credentials for personal gain.

Example of impersonator actions	▸ An individual who poses as a vendor to divert a payment. ▸ An individual who uses stolen identities to receive a fraudulent payment. ▸ An individual who poses as an employee to authorise a transaction.
Red flags to look out for	▸ Email communication that does not sound like typical emails you may have received from company executives in the past. ▸ Multiple funding applications from the same IP address. ▸ Email request demanding urgent payments to be made.
Countermeasures to support identity security and authentication:	▸ Governance, leadership, and culture - Ethical culture ▸ Prevention - Identity verification - Automatic prompts and alerts - Parameters and limits - Fraud awareness training ▸ Detection - Verify information received - Fraud detection software ▸ Response - Recovery and debt management processes

The Corruptor

- ✓ The Corruptor abuses their position of entrusted power to gain a benefit for themselves or another person.
- ✓ This might involve negative incentives such as threats or intimidation, or positive incentives such as bribes

Example of corruptor actions	▸ Public officials who misuse their position of power to receive extravagant gifts. ▸ Public officials who misuse their position of power to award government contracts. ▸ Public officials who manipulate a process to pay a relative or friend more than other similarly suited people.
Red flags to look out for	▸ Purchasing of inappropriate goods or services with no obvious business need. ▸ Over-inflated invoices or invoices that cannot be matched to any output. ▸ Continued acceptance of sub-standard goods or services despite complaints being made
Countermeasures to support probity, information security and oversight	▸ Governance, leadership, and culture - Fraud governance ▸ Prevention - Integrity checks and suitability assessment - Segregation of duties - Fraud awareness training ▸ Detection - Tip-offs and protected disclosures - Internal audits or reviews ▸ Response - Fraud investigation policy

The Deciever

- ✓ The Deceiver makes others believe something that is not true to dishonestly gain a benefit for themselves or another person.
- ✓ This might involve providing false statements, deliberate misrepresentation or withholding facts or circumstances.

Example of deceiver actions	▸ An individual who misrepresents facts or circumstances to receive a benefit. ▸ An individual who withholds key information to get increased payments. ▸ A vendor who withholds critical information to influence the award of a contract.
Red flags to look out for	▸ Individuals who do not answer questions. Individuals do not like to lie and will usually try to avoid answering a question before answering with a lie. ▸ Lack of detail on application documentation, only providing the bare minimum information or some not at all. ▸ Withdrawal of an application when questioned for additional information.
Countermeasures to support honesty, integrity, information sharing and verification	▸ Governance, leadership, and culture - Ethical culture ▸ Prevention - Eligibility criteria - Fraud awareness training ▸ Detection - Verify information received - Fraud detection software ▸ Response - Recovery and debt management processes

The Enabler

- ✓ The Enabler knowingly or complacently enables fraudulent activity to dishonestly gain a benefit for themselves or another person.
- ✓ This might involve an individual who intentionally keeps themselves unaware of the circumstances to avoid responsibility.

Example of enabler actions	▸ An individual who approves an expense claim for another person knowing that the expense does not comply with the expense policy. ▸ An individual who approves a grant knowing that the applicant is using a false identity. ▸ An individual who processes a vendor invoice, knowing that the invoice includes fraudulent charges.
Red flags to look out for	▸ Email communication that does not sound like typical emails you may have received from company executives in the past. ▸ Multiple funding applications from the same IP address. ▸ Email request demanding urgent payments to be made.
Countermeasures to support clear and consistent requirements and processes	▸ Governance, leadership, and culture - Fraud governance ▸ Prevention - Eligibility criteria - Procedural instructions or guidance - Automatic prompts and alerts - Fraud awareness training ▸ Detection - Quality assurance checks ▸ Response - Recovery and debt management processes

The Exploiter

- ✓ The Exploiter uses something for a wrongful purpose to dishonestly gain a benefit for themselves or another person.
- ✓ This might involve misusing their position or privileges or dishonestly exploiting a vulnerability for personal gain.

Example of exploiter actions	▶ An individual who splits a purchase into smaller contracts to keep it within their delegated authority to benefit a vendor. ▶ An individual who accesses permission to change their salary in the payroll system. ▶ An individual who exploits vulnerabilities to apply for emergency relief when they know they are not entitled to receive it.
Red flags to look out for	▶ Staff who have systems access which is broader than what their role requires. ▶ Inconsistent head count numbers between staff count and payroll processing systems. ▶ Multiple change requests for vendor contracts.
Countermeasures to support oversight and transparency:	▶ Governance, leadership, and culture - Ethical culture ▶ Prevention - Access controls - Limit access for sensitive information - Protect data from manipulation - Segregation of duties - Fraud awareness training ▶ Detection - Fraud detection software ▶ Response - Fraud investigation policy

The Fabricator

- ✓ The Fabricator invents or produces documents that are false to dishonestly gain a benefit for themselves or another person.
- ✓ This might involve creating false invoices or other types of records for personal gain.

Example of fabricator actions	▸ An individual fabricates documents, for example property titles, to receive a mortgage for their business. ▸ A staff member fabricates receipts, for example restaurant receipts, to support a false expense claim. ▸ A trustee fabricates documents, for example financial statements, to qualify for funding.
Red flags to look out for	▸ An individual fabricates documents, for example property titles, to receive a mortgage for their business. ▸ A staff member fabricates receipts, for example restaurant receipts, to support a false expense claim. ▸ A trustee fabricates documents, for example financial statements, to qualify for funding.
Countermeasures to support information sharing and verification	▸ Governance, leadership, and culture - Fraud governance ▸ Prevention - Protect data from manipulation - Parameters and limits - Fraud awareness training ▸ Detection - Verify information received - Fraud detection software - Automatic detection software ▸ Response - Fraud investigation policy

The Organised

- ✓ The Organised are a group of people who use a combination of sophisticated methods, in a planned and coordinated way, to dishonestly gain a benefit for themselves.
- ✓ This may involve using professional facilitators and service providers to help or facilitate their criminal activities.

Example of organised actions	▸ An individual that collaborates with multiple people to submit fabricated documents to secure fraudulent mortgages. ▸ A group of people that collaborate with an accountant to falsify business records to receive grant funding. ▸ A group of people that collaborate with individuals to use stolen identities to apply for funding.
Red flags to look out for	▸ A vendor that was created shortly before or after the contract was awarded. ▸ Excessive amount of missing information about applicants who received funds. ▸ Procedural or computer-system inquiries or transactions that are inconsistent with the user ID's normal duties.
Countermeasures to support information sharing and strategic collaboration	▸ Governance, leadership, and culture - Fraud governance ▸ Prevention - Parameters and limits - Fraud awareness training ▸ Detection - Verify information received - Fraud detection software ▸ Response - Recovery and debt management processes

COUNTER FRAUD CENTRE

Tauārai Hara Tāware