



SERIOUS FRAUD OFFICE

Te Tari Hara Tāware

MANDATE-FRAUD

WHAT IS IT AND HOW CAN IT BE PREVENTED?

WHAT IS MANDATE FRAUD?

Mandate fraud typically occurs when an agency is deceived into changing a regular payment mandate (such as a direct debit, standing order or bank transfer) by someone purporting to be an organisation or individual it makes regular payments to, such as a supplier of goods or services. It could also relate to the payment of membership or subscription fees. It generally involves the changing of account details for supplier or customer accounts in order to divert funds. Once the new account details are in place, any subsequent payment will not reach the true supplier because it is automatically diverted to the fraudster.

CONTENTS

WHAT IMPACT COULD COVID-19 HAVE ON MANDATE FRAUD?	02
HOW THE FRAUD WORKS	03
MANDATE FRAUD CASE STUDIES	04
HOW TO SPOT IT	05
HOW TO PREVENT IT	06

IF YOU THINK YOU HAVE BEEN TARGETED

Immediately report the issue to the person within your organisation responsible for risk, assurance or fraud prevention.

WHAT IMPACT COULD COVID-19 HAVE ON MANDATE FRAUD?

Many public sector agencies have had to rapidly adapt to changes in their working environments to deal with the COVID-19 event. These changes include:

- working remotely outside usual controls
- changes to established payment processes including an emphasis on paying suppliers quickly
- organisations taking on new types of payment obligations
- merging and reprioritisation of usual tasks
- new staff moving into payment roles.

As noted earlier, typically mandate fraud occurs when someone contacts an organisation with an urgent request to change a direct debit, standing order or bank transfer mandate, by purporting to be from a genuine supplier to whom regular payments are made. If the organisation accepts the fraudulent request, the payments are then diverted into the criminal's bank account. The large amount of funds flowing as a result of the government response to COVID-19, together with changes to normal processes noted above, will make this type of fraud extremely attractive to criminals.

Another common form of mandate fraud to be aware of is known as CEO/payroll fraud. This occurs where the fraudster requests changes to payroll bank account details. This type of fraud typically occurs when an email is sent to an organisation from a criminal purporting to be the organisation's CEO (or a senior manager) with instructions to change bank account details of the person they are impersonating. The criminal will request that funds are transferred as a matter of urgency to the alternative bank accounts.

The member of staff receiving the email will feel pressured to comply due to the apparent seniority of the sender and the urgent nature of the email. The fraudster may also use the seniority of the person they are impersonating to request that a supplier's bank account details are changed urgently to divert funds to the fraudster's account.

In both scenarios, the fraudster is hoping that normal controls and processes will be less strictly observed because of COVID-19.

During the COVID-19 pandemic, the urgent nature of the above requests are likely to appear more pressing and convincing. It is therefore vital that public sector managers and staff are particularly vigilant when paying suppliers and staff during this time, as New Zealand has already experienced cases of mandate fraud and it is particularly attractive to criminals as it represents a low risk enterprise with the prospect of high rewards.

The experience of other jurisdictions has also indicated that the COVID-19 event is likely to result in more attempts at mandate fraud.

HOW THE FRAUD WORKS

Criminals will gather information which is then used to impersonate suppliers, senior employees or customers from various organisations and individuals. Methods include:

- gaining inside knowledge, including from corrupt staff
- accessing publicly available contract information including publicly announced contracts and online logs of supplier contracts
- conducting online research about the targeted organisation, their activities and identifying key staff
- direct contact to gain information from unsuspecting employees, which may include telephoning staff at organisations to gain information about their procedures.

Once information is gained a number of methods may be used to gain control of an account and benefit from unauthorised payments. Fraudsters may request an update in account details through:

- telephone
- letter or fax
- email
- a combination of these.

Changes requested by fraudsters may include:

- changing bank details in a direct debit
- a payment to be made over the phone via credit card
- changing an employee's bank account details for their salary.

||| *Mandate fraud represents a low-risk enterprise for the criminal with the prospect of high rewards.*

MANDATE FRAUD CASE STUDIES

Example 1

A New Zealand company had a supplier in China they used regularly. Fraudsters obtained enough information about the Chinese supplier to imitate their emails, including using a very similar email address, and even copying the signature in the email. Fake invoices were sent to the New Zealand company, at a time when they were expecting to receive invoices from the supplier. As a result the invoices were paid to the fraudster's account, resulting in losses of over \$300,000.



New Zealand case studies of mandate fraud reflect examples already seen overseas.

Example 2

A fraudster inserted themselves into an email exchange between a public agency and a customer, with whom the agency was finalising a grant claim. The fraudster instructed the agency to change the bank account into which the claim was to be paid. However, at this point the agency's internal controls caught them out before any money was transferred to the fraudster. This detection was achieved by contacting the instructor offline using contact details already held for that customer, instead of the contact details on the electronic source, to validate the legitimacy of the instruction. The customer denied sending the instruction, which prompted the agency to investigate their systems and detect the fraudulent attempt. This type of example is particularly relevant in the event of an emergency, such as the COVID-19 pandemic, where agencies are responsible for the payment of significant sums of money towards the emergency response effort.

HOW TO SPOT IT

Mandate fraud can occur in different ways, but some common methods to be aware of include:

- Direct targeting and grooming or manipulation of individuals to induce them to reveal confidential information.
- A telephone request is received where the caller is suggesting some urgency in making a change to a supplier's bank account details.
- An email request is received from an unknown email account that is not recorded on the organisation's records.
- An email is received where a minor amendment has been made to the sender's address details, giving the impression it is a genuine contact email address at first glance. For example, the genuine address is joebloggs363@mail.com but the fraudulent email came from joebloggs36@mail.com. Staff should always check the authenticity of an email received from a supplier (e.g. the domain name) by using established supplier contact details already held on file.
- A written request is received in the form of a letter or invoice that does not contain the supplier's logo or the logo may be less sharp or slightly blurred (this would most likely be a scanned copy of an original document which has been counterfeited).



Public sector organisations should be alert to the different methods used by fraudsters to commit mandate fraud.

HOW TO PREVENT IT

Mandate fraud can involve sophisticated techniques. Those attempting it have often harvested information on their targets and may use well-honed techniques to impersonate your suppliers. However, by being alert to the fraud risk and by ensuring you and your organisation follow some simple checks, you can significantly reduce the likelihood of falling victim to it.

- Organisations should periodically confirm supplier information held on file, including bank account details, registered address, email address, company registration number, GST number, or the name of the key contact at the company.
- All staff should take caution when providing sensitive company information, by phone or other means, especially contract and account information.
- Use existing payment systems and partners if possible.
- Make sure to review and adhere to existing information security policies such as clear desk, staff vetting, and internal and external financial

IF YOU THINK YOU HAVE BEEN TARGETED

Immediately report the issue to the person within your organisation responsible for risk, assurance or fraud prevention.

controls. Even in a working from home (WFH) situation, employees should still adhere to information security policies relating to their online systems and follow established protocol.

- If unsure, contact your supplier using records in your system (not on the communication requesting the change) to check the veracity of the request.
- Public sector organisations should continue to ensure that authorisation and monitoring procedures are in place for the creation and changing of bank details and monitoring of payments, and that employees are aware of these processes and know how to use them.
- Implement processes for managing payments over a certain amount. For example, the process could involve needing two people in your organisation to review or sign off on an invoice over a certain amount.
- Ensure security systems are in place to protect information stored online and in email accounts, for example two-factor authentication for remote access email accounts. Check that these are working properly for WFH employees.
- Look at opportunities to train staff on social engineering techniques that could be used by an attacker to commit mandate fraud (social engineering is the psychological manipulation of people into divulging confidential information they would otherwise not provide).
- Always issue receipts or remittance advices to suppliers so they know when a payment has been made.
- Report suspicious activity/transactions to your organisation's bank as soon as suspected.
- Alert staff to all unsuccessful frauds so they can be prepared for repeat attempts.

About the Serious Fraud Office

The SFO is the lead law enforcement agency for investigating and prosecuting serious financial crime, including bribery and corruption. Detection, investigation and prosecution of serious and complex financial crime, including corruption and bribery, is at the heart of what we do.

We are also committed to preventing these crimes. If you require further information about this toolkit, or if you would like assistance in relation to the design, implementation or operation of a specific relief programme then please contact the Serious Fraud Office at **counterfraud@sfo.govt.nz**.