Government Counter Fraud Function

GOV.UK/coronavirus

COVID-19 Mandate Fraud

Introduction

The threat from mandate fraud has increased during the COVID-19 response. This could result in organisations losing substantial amounts of money that will be difficult to recover. However, whilst mandate fraud is becoming more sophisticated, it is entirely preventable if your organisation is aware and takes the threat seriously.

The threat from mandate fraud is increasing because the public sector has had to rapidly adapt to new ways of working and is necessarily spending money quickly to deal with COVID-19. This has created new vulnerabilities, which criminals are seeking to take advantage of. This type of fraud carries low risk and potentially high rewards for criminals.

We have already seen instances of attempted mandate fraud around the COVID-19 response. We should not underestimate the sophistication of this fraud. It is not just people emailing to ask for bank accounts to be changed, those attempting it have often harvested information on their targets and use sophisticated 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.

Mark Cheeseman, Director Government Counter Fraud Function

What is Mandate Fraud?

- It is a fraudulent request to change a direct debit, standing order or bank transfer mandate in order to divert payments or to create new payments.
- It can affect customer, supplier or employee bank accounts.
- It is also known as creditor fraud, payment diversion fraud or supplier account takeover fraud.

How Does Mandate Fraud Happen?

Criminals will gather information about your suppliers, customers or senior employees from different sources to make them look legitimate when contacting your organisation. This can vary from simple to in-depth information. This helps them to impersonate organisations and individuals convincingly.

They will make a request to change the bank details by a number of methods:

Telephone: criminals will impersonate a genuine supplier and often call with an urgent or time critical reason to get changes made in a hurry.

Written requests (letter or fax): criminals will create fictitious but convincing letters or faxes which quote publicly available information such as company registration and director details.

Email requests: criminals will 'spoof' email addresses and include fabricated but convincing content to appear legitimate.

How to Prevent Mandate Fraud

- Be alert and suspicious of any requests to alter bank details - criminals are targeting us.
- Be especially vigilant with changes close to a payment date - or changes closely followed by invoices.
- Check contact details contained within phone calls, letters or emails received and validate all requests for bank account changes using established contact details.
- Report unexpected or unusual emails that have unknown links or attachments.
- Ensure that a senior member of your finance team reviews and formally authorises the change of bank account details.
- Review bank statements and payment records regularly and report anything suspicious to your bank immediately.
- Avoid disclosing sensitive information about your suppliers to unknown third parties.
- Shred confidential documents before throwing them away
- Assess your security policies on a regular basis and ensure that all staff are briefed and trained to spot potential fraud.

You can contact the Government Counter Fraud Function by emailing **covid19-counter-fraud@cabinetoffice.gov.uk**

Local Authority Case Study:
Bank Account Details Changed

A Local Authority had numerous construction contractors for the refurbishment of schools. They received an apparently genuine letter from one of these contractors stating they had changed their banking details. No checks were conducted and the bank details were updated. Within a week, two payments totalling over £2 million were transferred to a bogus bank account.

COVID-19 PPE Mandate Fraud Case Study

An international supplier of personal protective equipment had their email compromised by organized criminals, who then used this data to contact the UK supplier, and request a change of bank account details for payment prior to shipping. The UK supplier was about to pay for vital equipment on its way to the NHS. The UK supplier was suspicious and sought advice. Their action prevented the fraudulent payment being processed. The details were then shared which meant the intelligence could then be shared with other organisations to help prevent this type of fraud and increase vigilance.

Charity Case Study:
Spoofed Account

An accountant at a charity received a phone call from a male purporting to be from a high street bank. The fraudster's number was 'spoofed' to resemble the bank's phone number and the caller stated there had been attempts by a third party to access their account. The fraudster spent considerable time gaining the confidence of the accountant, even sending a plausible email that looked like it had come from the bank. The fraudster persuaded the accountant to download software which allowed the fraudster remote access to the charity's bank accounts. The accountant was convinced to provide login details for a second bank account. The fraudster told the accountant that both accounts would be subject to "ghost transactions" to test their security and the money would not actually leave the accounts. However, this was a lie and a six figure sum was transferred to numerous fraudulent accounts.

Look Out for Senior Impersonation Fraud

Senior impersonation fraud involves the impersonation of a senior employee with subsequent requests for transfers of funds or change of bank account details. It is a sophisticated fraud that plays on the authority of senior officials.

- An employee receives a phone call or email from someone claiming to be a senior member of staff – they ask for an urgent payment to a new account and instil a sense of panic. Criminals can hack a staff email account or use spoofing software to appear genuine.
- The criminal may pick occasions when the senior employee is on holiday, preventing the financial officer from checking the validity of the request.
- Advice: Be cautious about unexpected urgent requests for payment from a senior employee and always check the request in person if possible.

TAKE FIVE TO STOP FRAUD™

Criminals are experts at impersonating people, organisations and the police. They spend hours researching you for their scams, hoping you'll let your guard down for just a moment. Stop and think. It could protect you and your money.

STOP

Taking a moment to stop and think before parting with your money or information could keep you safe.

CHALLENGE

Could it be fake? It's ok to reject, refuse or ignore any requests. Only criminals will try to rush or panic you.

PROTECT

Contact your bank immediately if you think you've fallen for a scam and report it to Action Fraud.

If You Suspect Mandate Fraud

1. **Notify your bank immediately**
2. **To report a crime or incident, please call Police Scotland on 101 or 999 in an emergency**

The Government Counter Fraud Function has set up the COVID-19 Fraud Response team to help public bodies reduce the threat and harm from fraud during the response to the COVID-19 pandemic. They are helping organisations understand the risks they face, sharing information on fraud threats and working with public bodies to implement countermeasures to reduce fraud.

You can contact them for more advice by emailing: **covid19-counter-fraud@cabinetoffice.gov.uk**