# Bank Mandate Fraud

## 1. Introduction - what is mandate fraud?

1.1 Mandate fraud, sometimes known as 'payment diversion fraud' or 'business email compromise', occurs when someone purporting to be from a genuine supplier contacts the council with a request to change bank account details that payments are made to. If the request is actioned, the payments will then be made to the fraudster's bank account.

1.2 This type of fraud is targeted at both the public and private sector as well as individuals. The National Crime Agency has stated that in the year to September 2021 (these are the most current figures reported) there were reported losses of around £152m and over 4,600 individual cases.

1.3 Criminals are very sophisticated in hacking accounts and compromising emails for mandate fraud, sometimes spending many weeks or months harvesting data or social engineering prior to changing the bank account details. As in the case that targeted the council, a business or supplier's emails are compromised by the fraudsters who then have control of them. Therefore, the fraudsters can use the company's actual email address rather than an address which is a close copy and therefore much harder to detect.

1.4 The council was subject to such an incident in early July 2023 resulting in a payment of approximately £52,000 being made to a fraudster instead of the intended supplier. This is the first time that the council has been defrauded in this way, and there are recent examples of where controls have prevented such frauds.

1.5 This Appendix is intended to give sufficient information to inform about what happened and actions taken to mitigate the risk of fraud recurring without providing specific details that could identify parties involved or give potential fraudsters information that could be potentially useful to them. There is an accompanying blue paper (not for publication) which contains more specific detail which will be reviewed by elected members.

1.6 This fraud incident was previously reported in the Internal Audit Mid-Year Report in November 2023. This report sets out additional information regarding the fraud to further inform members.

# 2. Circumstances around the fraud

2.1 In late June and early July 2023 a series of e-mail communications were received from a known supplier and verified e-mail address. These communications included a change of bank details and an invoice.

2.2 Unfortunately, although the email was from the correct and verified address, our supplier had been the subject of a sophisticated cyber-attack and at this stage an additional internal process to verify bank account changes was not correctly followed and as a result, this invoice was included in a payment run in early July.

2.3 Our banking partner notified us of a potential fraud whilst the payment was in transition and although staff responded promptly at this point contacting the supplier to verify the bank change and then reporting to our banking partner that the payment should be stopped, our banking partner could not prevent the payment being made to the fraudulently provided bank account. There is further detail on this included in the accompanying blue paper (not for publication).

2.4 In this circumstance, once the payment was made, the risk of failure to recover the fraudulently obtained money sits with the payer.

# 3. What actions were taken when the fraud was discovered?

3.1 Upon discovery of the fraud, the immediate steps taken were to contact the receiving bank to seek recovery, the police (through their Action Fraud reporting centre) and the issuing bank to review potential avenues of escalation. All other potential payments to the supplier were put on hold. This was all done on the day that the fraud was uncovered.

3.2 Following this initial response communication continued with the supplier, the banks, law enforcement, legal advisors, e-mail providers and other connected agencies in order to clarify what had occurred and to seek recovery of the amount paid.

3.3 Internal audit carried out an investigation which covered the circumstances around the fraud, what controls are in place to assist in the prevention of mandate fraud, where these controls had failed, and what actions should be taken to reduce the risk of any such further frauds. A report was issued to the S151 Officer covering these areas on 10 July 2023. Internal audit also confirmed that staff were not involved in perpetrating the fraud.

3.4 Further follow up work was also undertaken by internal audit and reported on to the S151 Officer in November 2023. This work confirmed that a number of actions, as set out below in paragraph 4.1, had been taken to reduce the risk of any similar future fraud. Further work will be

undertaken by internal audit before the Internal Audit Annual Report 2023/24 is presented to the Performance and Audit Scrutiny Committee in May 2024 to consider whether controls are operating as intended.

3.5 The fraud was reported to Action Fraud which is the UK's national reporting centre for fraud and cybercrime where any fraud involving being scammed, defrauded, or subject to cybercrime should be reported. Action Fraud is run by the City of London Police on behalf of all UK police forces.

3.6 The external auditors were also informed of the fraud.

3.7 Further information on actions taken is covered in the exempt paper.

# 4. What has been done to reduce the risk of future bank mandate fraud?

4.1 Actions taken include the following:

- the intranet fraud awareness page has been revised and a news item published on the intranet
- the service and staff involved were spoken to and training given.
- all Service Managers have been separately reminded in writing of bank account change requirements
- mandate fraud awareness guidance has been added to the finance team pages on the intranet including the process to follow for bank account changes
- a training programme has been delivered to invoice processors to emphasise and reinforce required internal control processes. This was accompanied by e-mail and intranet reminders including new training video resource from the council's bank
- the required additional checks to be carried out, and responsibilities, within the finance team have been documented to confirm a more robust check of bank mandate changes
- A form has been created on the accounting system to record the checks completed by the finance team to validate a bank account change
- a report has been set up within the accounting system to highlight any account changes in our supplier base. This will be run by the finance team and used to validate checks that have been performed by the commissioning service
- awareness of fraud scams has been reinforced within the finance team