Bank Mandate Procedures
North Yorkshire Fire and Rescue Service
Memorandum Report

For: Chief Accountant (Enable NY)
Status: Final
Date Issued: 6 March 2022

Veritau

Introduction

1 Mandate fraud occurs when someone contacts an organisation with a request to change a direct debit, standing order or bank transfer mandate by purporting to be from a genuine supplier from whom regular payments are received. If such actions are not identified then this could result in monies being diverted to the criminal's bank account.

2 Within the public domain there is a lot of financial and other information available which leads to public sector bodies having an increasing risk to such fraudulent activities. In addition, Veritau has seen an increase in the number of local attempts to change supplier details and divert payments into bank accounts controlled by criminals.

3 Having strong controls in this area is very important to all organisations, including North Yorkshire Fire and Rescue Service (NYFRS). Given the increase in local incidence of attempts to fraudulently change supplier details we discussed and agreed with the service's s151 officer to complete some targeted work reviewing the payment controls in place at NYFRS.

Objectives and scope

4 The purpose of the work was to provide assurance to management that procedures and controls in place to prevent fraudulent changes to suppliers' bank account are appropriate.

5 Work involved a meeting between the Chief Accountant (Enable NY) and the Management Accountant (Finance), with an Internal Auditor and Counter Fraud Investigator from Veritau, on Wednesday 17 November 2021.

Findings

6 In advance of the meeting the Management Accountant had sent Veritau a written description of the system in place to process bank account changes for suppliers. A copy of this description is included below.

Bank Account Check.xls

7 Our Counter Fraud Investigator (CFI) compared these local arrangements to the processes and controls that help to minimise the chances of a fraudulent change being made. We concluded there were no weaknesses, subject to these local arrangements being consistently and appropriately followed.

8 The CFI provided some extra background and insight into the type of issues we are increasingly seeing. Fraudsters are now submitting changes to contact details as a pre-emptive measure to subsequently requesting a change of bank details. These actions can result in the change of bank

details being verified using the previously supplied false contact details. We are also aware of email conversations being hacked and changes to bank details being requested within the email exchange. It was imperative to check any changes to a suppliers details, not just bank details, directly with the supplier by using pre-existing contact details.

9 A quick reference guide was shared following the meeting which officers said would be distributed to all relevant staff at the next team meeting.

Overview provided
to NYFRS November

10 Officers explained that manual records of each change made and the checks made, including who processed the change, and who authorised it, are retained. Only specific officers (six in total) can process such changes, so they felt confident all changes will have been correctly processed following suitable checks being made.

11 We asked whether the service would have assurances all changes in the creditors system had been processed using the prescribed system. Officers explained there was always a risk of non-compliance with manual procedures of this type. In respect of bank mandate fraud NYFRS officers regularly discuss cyber-security in team meetings and share intelligence passed on by audit or other parties.

Next steps

12 Our draft report was issued in December 2021. Officers agreed to complete some work to help provide some additional insight into the compliance with the internal procedures on changing bank details. Specifically this was to involve:

- obtaining the number of suppliers paid from 1 December 2020 to 18 November 2021.
- interrogating the payments system to determine how many bank accounts have been changed as documented in the system during this period
- Comparing the payments system information with the local records held showing the changes recorded as approved (to determine if there are any changes which have not been approved) and further investigate if appropriate.

13 Information is required to be gathered internally (on suppliers) and from North Yorkshire County Council's Exchequer Service (payments system) which is currently ongoing. Once completed this will help inform the service as to the completeness of the application of the local procedures and the extent to which periodic future checks of the same type may need to be completed.