North Somerset Council

Report to the Audit Committee

Date of Meeting: 25th April 2024

Subject of Report: Counter Fraud Annual Report

Town or Parish: None

Officer/Member Presenting: Peter Cann, Audit West

Key decision: no

Recommendations

The Audit Committee is asked to note the Counter Fraud Annual Report.

1. Summary of Report

This is an update report to outline the main counter fraud activity that took place during the 2023-24 financial year.

2. National Picture and Emerging Fraud Risks

2.1 The CIPFA Fraud and Corruption Tracker (CFaCT) survey is the definitive survey of fraud and corruption activity in local government. It tracks the level of fraud and corruption local authorities have detected, the number of investigations undertaken and the types of fraud encountered.

The CIPFA Tracker Report was last published in 2020 and detailed the main themes for national fraud indicators within Local Government. This can be accessed via the CIPFA website:
https://www.cipfa.org/services/cipfa-solutions/fraud-and-corruption/fraud-and-corruption-tracker

The tracker report is supported by the National Audit Office (NAO) and the Local Government Association (LGA). The annual financial loss to fraud in the UK public sector was last estimated to be £40.3bn annually, with £7.3bn of this total being lost in local government.

2.2 **Internal Audit Coverage of Key Fraud Risks**

Key fraud risks specific to Local Authorities continue to include:
- Council Tax Fraud
- Disabled Parking Concessions (Blue Badge)
- Business Rates
- Housing Fraud

Procurement Fraud is also an increasing risk and coverage of this was completed in 2023/24 (Compliance with Council Procurement Process) with two further audits planned in 2024/25 (Procurement Act 2023 and Compliance with Changes to CSOs).

Additional audits completed in 2023/24 that are linked to key Local Authority fraud risks included reviews of Council Tax and NNDR (Business Rates) and Housing (Lettings Service).

Further work proposed within the 2024/25 Internal Audit Plan is to include a review of the 'Tell Us Once' service, which spans across Blue Badges and is an important fraud deterrent. This audit is in part included due to the findings within the recent NFI exercise (see section 3).

Cyber Fraud continues to be a significant challenge across the landscape nationally. Audit reviews of Cyber Security (including staff awareness) and Ransomware are included as part of the 2024/25 planned programme of work in order to provide assurance over the effectiveness of controls in these areas.

2.3 Fraud Prevention Networks and Identified Fraud

The Internal Audit Service obtains information regarding known and emerging fraud risks from a number of sources, organisations and professional bodies. One of these is the National Anti-Fraud Network (NAFN). NAFN are one of the largest shared services in the country, managed by, and for the benefit of its members, and is hosted by Tameside MBC. Currently, almost 90% of local authorities are members, including North Somerset Council.

As part of the above arrangement with NAFN, Internal Audit has a process in place for onward sharing and discussion of NAFN alerts. This process is in place to raise awareness across the Council of local and national fraud risks and to highlight or investigate areas of known concern.

A fraud alert was received in December 2023, which Internal Audit shared the with the Council's Revenues and Benefits team. The alert was in relation to a Council Tax scam that was cross border with multiple authorities affected. The Alert was sent by NAFN for reference and with a request to review names, addresses and bank accounts known to be used in this fraud activity against Council records to ascertain if there was any similar activity impacting North Somerset Council.

In early 2024, the Revenues & Benefits Client Lead at the Council contacted Internal Audit to report that a match of name had been identified on Council records and that a successful fraud attempt against the Council had been discovered. The fraud had occurred when contact was made with the Council online and also on the phone by somebody claiming to be a customer that was liable for payment of Council Tax at a property. A Council Tax payment was made on a fraudulent credit card, but then later refunded into a different bank account. The total identified financial loss incurred as a result of this fraudulent activity is £437.56.

Further detailed work will be undertaken in 2024/25 (as part of scheduled fraud prevention activity) to establish whether there any further/ revised controls that need to be put in place to reduce the risk of this happening again in future. Meanwhile, the fraud has been reported to NAFN and also to Action Fraud.

3. National Fraud Initiative (NFI)

3.1 The Internal Audit function also carry out other anti-fraud activity, such as co-ordinating the National Fraud Initiative (NFI) on behalf of the Council's Section 151 Officer.

3.2 The NFI is a Cabinet Office initiative, matching data from a large number of public and private sector organisations. These organisations provide data from their systems as prescribed by the Cabinet Office. The data is then matched and data matching reports are made available for each participating organisation to review. It is for each organisation to make the necessary enquiries and any identified fraud is recorded within the NFI system to enable the effectiveness of the initiative to be monitored.

For Local Authorities such as North Somerset Council, example data sets for matching purposes include (but are not limited to); Housing Benefit, Council, Payroll, Adult Social Care Personal Budgeting and Disabled Parking (Blue Badges).

3.3 Results from the Latest NFI Exercise

The results from the in-year exercise have given estimated savings as follows:

Report title	Total matches	Fraud/ errors	Outcome	Cabinet Office Estimates	Total
Housing Benefits	46	0	£0.00	£0.00	£0.00
CTax Reduction Scheme	220	3	£519.35	£116.16	£635.51
Payroll	29	0	£0.00	£0.00	£0.00
Blue Badges	808	185	£0.00	£120,250	£120,250
Waiting List	135	0	£0.00	£0.00	£0.00
Creditors	1377	1	£40,544.52	£0.00	£40,544.52
Procurement	20	0	£0.00	£0.00	£0.00
TOTAL	**2635**	**189**	**£41,063.87**	**£120,366.16**	**£161,430.03**

i) Blue Badges – Estimated Savings £120,250

The Blue Badges matches were in relation to service users that have passed away but the badges remained active. It should be noted that the savings are based on Cabinet Office estimated national 'averages' for the worth of a badge (street value of badges are worth much more in London for example). There is no confirmation that any of the badges have been used inappropriately, as a result the estimated savings provided by NFI might not reflect actual savings to the council.

The matches are a result of the Blue Badges team not being informed when a service user passes away, and as a result the badges are not being cancelled. It should be noted that evidence was provided in-year that all of the notifications received through the councils "Tell Us Once" system had been processed by the Blue Badges team. However, an audit review of this system is proposed as part of the 2024-25 audit plan in order to understand if there are any issues in this area which might mean that information isn't getting shared across departments as it should be.

ii) Duplicate Payment - £40,544.52

A separate audit review of the 'root-causes' of duplicate payments was completed during 2023/24 (see 4.2) and this included investigation as to how the overpayment of

£40,544.52 identified in the NFI exercise was able to occur. Essentially, it was confirmed that this payment was not picked up as would usually happen with a duplicate purchase order number and value, due to the fact that the contract was a value order.

With a contract value order, a company can send in multiple invoices across the year against one purchase order number. The purchase order number does however have a financial limit set against it, so once the limit is reached then subsequent invoices would be rejected. Since at the time of the duplicate invoice coming in the limit had not been reached it was accepted.

A recommendation was made (and accepted) that the supplier was to be added to a watch list on the supplier master file. This would ensure that when any future invoices from the company are received, staff will be prompted about the issue identified in order to improve controls and prevent a recurrence. In addition, enhanced duplicate payment testing by Accounts Payable has been recommended.

The Audit Committee are advised that the duplicate payment of £40.544.52 has been recovered.

4. Internal Audit Targeted Work and Investigations

4.1 Internal Audit Planning and Reviews

The risk of Fraud is considered during all internal audit planning activity and members can see evidence of this throughout this annual report. This includes thought right from initially building the Annual Audit Plan (i.e. the audit reviews planned to be carried out during the financial year) through to considering the objectives, fraud risks, controls and focus of each review to be carried out, i.e. each individual work programme. As described in this report, work will be carried out in 2024/25 on known key fraud risk areas, including Cyber Fraud, Procurement, Blue Badges (via 'Tell Us Once' review), as well as NFI and Data Analytics reviews.

4.2 Data Analytics

Data analysis and data matching are important tools for identifying fraud and error in local government. The Fighting Fraud and Corruption Locally Strategy for the 2020s recommends that local authorities should share data across its own departments and engage in the use of data analytics as a key response to fraud.

As well as participating in the National Fraud Initiative (see section 3), Audit West wishes to support effective data analysis with the use of existing information that the authority already holds. Therefore, internal data matching takes place regularly throughout the year and this is partly completed via IDEA – an internal audit data analytics software tool.

The work completed in 2023/24 did not identify any fraud, however, it did identify 84 potential duplicate payments totalling £29,637 which had already been picked up by Accounts Payable and already cancelled or reversed. One further duplicate payment was identified to the value of £228.96 which had not previously been picked up but has now been recovered.

The internal matches were completed primarily on data from the payroll and creditor system. The main checks that took place and findings that were identified as follows:

No	Match type	Fraud or Error Identified	Value of Fraud /Error	Total matches identified	Comments
1	Duplicate payments by invoice number, supplier I.D. and amount.	No	n/a	84	A total of 84 potential duplicate payments were identified from the data match. The total value of the matches was £29,637. However, the average value was only £705, due to the highest value invoice being for £20,000. The matches were investigated, and it was identified that that the payments had already been identified by Accounts Payable and had been either cancelled off or reversed. As a result, no outstanding duplicates remained.
2	Duplicate payments by invoice number and amount.	1 error	£228	136	A total of 136 potential matches were identified from the initial data matching. For 1 invoice for £228.96 was identified as being a duplicate, and accounts payable have confirmed that the money has been recovered. No other issues of genuine duplicates were identified, with the matches either being separate payments or having previously been identified and corrected by accounts payable.
3	Supplier gap detection - General Suppliers. Supplier gap detection - Ukraine Grant programme. Closed Covid-19 Suppliers.	No No No	n/a n/a n/a	8 7 2	A total of 8 gaps were detected in the general supplier file. All the gaps had been previously identified and were the result of issues when the Agresso system was originally set up. No new gaps have been detected. A total of 7 gaps were detected in the supplier numbers for the Ukraine support payment, no payments have been made and the suppliers were never set up on the system. All of the suppliers that had been set up to received Covid-19 payments had been closed down on the system, with the exception of two which were identified as part of the audit. The two open Covid suppliers have subsequently been closed.
4	Duplicate suppliers by bank account.	No	n/a	162	A total of 162 potential matches were identified. These were reviewed and legitimate reasons for the matches exist.
5	Payroll match by	No	n/a	19	A total of 19 matches were identified relating to staff that had duplicate bank details. The matches were reviewed,

	bank account.				and steps taken to ensure that the employees were real. The issue is primarily the result of staff using joint bank accounts with their partner.
6	Duplicate National Insurance Number.	No	n/a	0	No staff were identified as having duplicate national insurance numbers. Staff with multiple jobs were reviewed. No issues with sickness or exceeding maximum hours worked were identified.
7	Over retirement age checked. Employees under the age of 18.	No No	n/a n/a	60 3	A total of 60 employees were identified as being over the retirement age. There is no obligation for staff over retirement age to retire. A review of the staff identified that they were employed mainly in casual or part time roles. A total of 3 employees were identified as being below the age of 18. One employee was 15 the other two 17 years old. All of the roles were casual and appear to be compliant with guidance for employment of individuals under 18.
8	Creditors to payroll by bank details.	No	n/a	116	A total of 116 transactions were identified. A sample of transactions were reviewed, and no concerns were identified.

Root Cause Analysis

A root cause analysis review was conducted on the duplicate payments that had been identified either as part of the Data Analytics audit or as part of the National Fraud Initiative. This review sought to identify the reason(s) why potential duplicate payments were not identified prior to the NFI and data analytics work being undertaken, or where they were already identified, work was completed to identify the reasons why the duplicate occurred, how it was detected by Accounts Payable, and if steps can be taken to reduce the number of potential duplicates.

From the analysis conducted the duplicates can be separated into three categories.

i) Contract Order – see 3.3. (ii)

ii) Cheque Payments - Whilst the majority of payments made by the Council are via BACS, the Council still makes some payments via cheques. When cheques are then cancelled due to the supplier being paid through another method, this identifies as a duplicate payment. The Council raised a project to reduce the number of cheques being issued to pay one off sundry payment via cheque and instead pay them through the BACS system and this has recently gone live, hence an expected reduction in cheque payments in 2024.

iii) Incorrect Supplier ID - Matches were identified where the incorrect supplier number had been issued. This can occur when the incorrect supplier ID is selected, as in some instances, the suppliers have the same or similar names. This is usually for companies that want payments to be made to different accounts, and as a result, the supplier will be set up as two different suppliers

so that payments can be made. However, if the wrong supplier ID is selected, then this could initially go undetected, since the name and address of the company are likely to be the same or similar.

The Accounts Payable team are responsible for ensuring that payments are properly authorised in compliance with the councils' procedures. Individual manager and budget holders are responsible for approving the payments and ensuring that they are legitimate.

4.3 Investigations

During Internal Audit investigations, the themes of prevent and pursue as recorded in the Anti-Fraud and Corruption Strategy are the focus of the work of the Auditor. The key objectives are to:

a) Identify the breakdown in controls and correct this to avoid further losses
b) Collect evidence to be able to pursue responsible individuals, i.e. through criminal prosecution or a disciplinary route.

There was one main Audit investigation in the 2023/24 financial year which was previously reported in-year to the Audit Committee. The investigation concerned a whistleblowing allegation made, the result of which concluded that the allegation could not be fully substantiated.

4.4 Fraud Reporting

In the financial year 2023/24, a total of 25 potential fraud referrals were received from the public through our dedicated fraud email address and referral form. The majority of the referrals related to areas such as Housing Benefit and Single Person Discount and were passed to the relevant area for action. We continue however to also receive reports of planning issues, as well as safeguarding concerns, within the referrals and in 2023/24 audits were undertaken within both of these service areas to give confidence that there were no underlying issues leading to these referrals.

4.5 Staff Training and Awareness

4.5.1 The Internal Audit service has continued to provide fraud information and awareness to staff throughout the year, with the staff newsletter 'The Knowledge' being a key channel of communication.

'International Fraud Awareness Week' fell between 12th – 18th November this year and a special article was published outlining all the key fraud prevention information that is available to officers, and detailing up to date information on the following headings:

- What is Fraud?
- Fraud and Local Government
- Why is Preventing Fraud Important?
- Who Commits Fraud and Why?
- Whistleblowing
- The Evolution of Cyber Fraud
- Our Strategy and Policies
- The Role of Internal Audit in Tackling Fraud
- Training and Resources

4.5.2 The audit service also produced articles for staff which covered the National Fraud Initiative; the new central Government 'Stop! Think Fraud' initiative; the emergence of QR (Quick Response) code fraud, and Whistleblowing.

4.5.3 The audit service has worked with the Inclusion and Corporate Development Manager team to transfer the content of online Fraud Awareness training onto the Council's new 'iLearn' system. Completion of this training is mandatory for all staff.

5. Strategy and Policy

5.1 Nationally, the Fighting Fraud and Corruption Locally 2020 document is the most recent counter fraud and corruption strategy for local government. It provides a blueprint for a coordinated response to fraud and corruption perpetrated against local authorities.

5.2 The Council's own Anti-Fraud & Corruption Strategy adopts the national strategy at a local level and is the "umbrella strategy" that brings together all fraud related policies. Its objective is to ensure that the Council is proactive in preventing and detecting fraudulent activities and corrupt practices and takes the necessary action to punish those involved and recover losses. The Council's Anti-Fraud and Corruption Strategy was refreshed, updated, and then approved in April 2022 by the Audit Committee.

5.3 Policies linked to the Strategy were also reviewed, updated, and approved in April 2022. These included the Whistle Blowing Policy, the Anti-Money Laundering Policy and Guidance, and the Anti-Bribery & Corruption Policy

6. Consultation

The Audit Committee is asked to note the Counter Fraud Update Report.

7. Financial Implications

There are no direct financial implications from this report which is focused on updates, however the Committee are asked to note the financial savings identified in the NFI exercise.

8. Legal Powers and Implications

There are no direct legal implications from this report which is focused on updates.

9. Climate Change and Environmental Implications

The council faces a wide variety of climate change and environmental impacts whilst delivering its many services to residents, some of which have a direct or indirect financial impact or consequence. These are referenced or noted, where appropriate, throughout the report.

10. Risk Management

It is recognised by Government that the current economic climate in the United Kingdom including the cost-of-living crisis have the potential to increase the risk of fraud and irregularity as never seen before in the Public Sector. Furthermore, as the Council makes continued cuts in its future budgets, it is essential that it continues to maintain strong defences against fraud and irregularity, directing its resources most effectively to mitigate the areas of highest risk.

11. Equality Implications

Embedded within the approach to fraud prevention is consideration of compliance with statutory guidance and regulations which includes those relating to equality and diversity.

12. Corporate Implications

There is a requirement to have a strategy which applies to all aspects of the council's business and has in place polices and processes to support the prevention and detection of fraud and corruption.

13. Options Considered

None.

Author

Peter Cann – peter.cann@n-somerset.gov.uk

Background papers

Internal Audit Update Report to Audit Committee, November 2023
2023/24 Internal Audit Plan – March 2023