Nottinghamshire County Council

ANNUAL FRAUD REPORT 2022/23

1. National Fraud Landscape

1.1. The CIPFA backed publication, ‘Fighting Fraud & Corruption Locally’ (FFCL), is the recognised counter fraud and corruption strategy for local government and was adopted by the Council in 2020.

1.2. The key fraud risk areas for local government were previously highlighted by the CIPFA Counter Fraud Centre (CCFC)’s annual ‘Counter Fraud and Corruption Tracker’ (CFaCT). The Council previously participated in this annually, however, the exercise has not been undertaken since 2019/20 and there is no alternative comparable data. Therefore, the latest reported figures for 2019/20 compared to 2018/19 financial year are as follows:

↓ Total value of fraud detected or prevented is down:

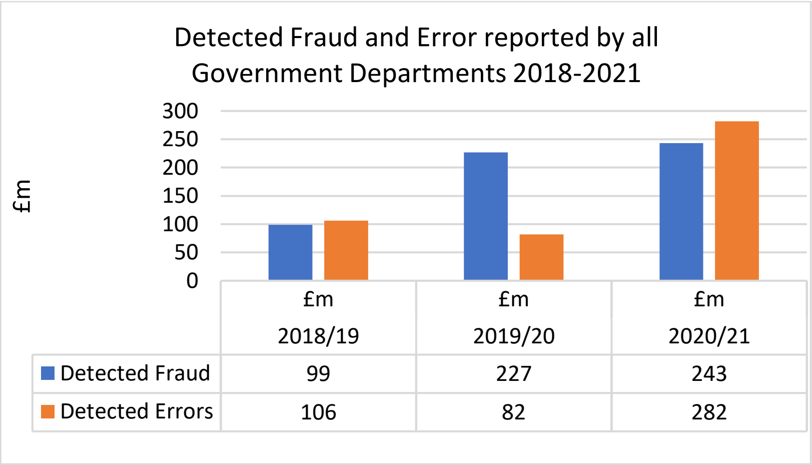
£239.4m in 2019/20 compared to £253m in 2018/19

↑ **Average value per fraud has increased to £5,090 compared to £3,600 in 2018/19**

↓ The number of frauds detected or prevented has decreased to 47,000 in 2019/20 from the 71,000 cases found in 2018/19

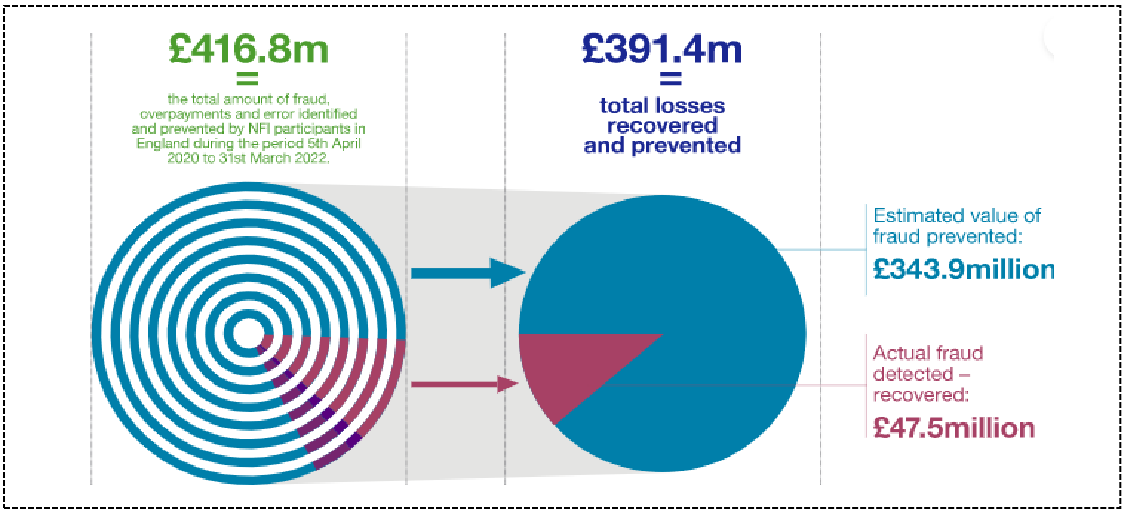
1.3. Whilst there are no local authority statistics, the UK government has published a Cross-Government Fraud Landscape Annual Report 2022 which reports upon levels of fraud and error across government departments for the 2020/21 financial year. This indicates there has been a rise in the levels of reported fraud and error in the public sector. This is in the context of increased levels of spending and fraud risk as a result of the pandemic.

1.4. The Government Counter Fraud Function estimates that in 2020, the level of fraud and error was between £33.2bn and £58.8bn outside of Covid-19 specific schemes. The incidences of identified fraud and error reported across the public sector since 2018 are as follows:


Detected Fraud and Error reported by all Government Departments 2018-2021

	£m 2018/19	£m 2019/20	£m 2020/21
🟦 Detected Fraud	99	227	243
🟧 Detected Errors	106	82	282

1.5. According to the Cabinet Office their National Fraud Initiative Report (NFI) December 2022, fraud is estimated to account for 40% of all crime committed across the UK. Matched data is used to help in the prevention and detection of fraud. It is reported that in the period 2020 to 2022, the NFI has enabled participant organisations to detect/recover £417m across England.



Source: NFI 2020 to 2022 Outcomes in England, Cabinet Office

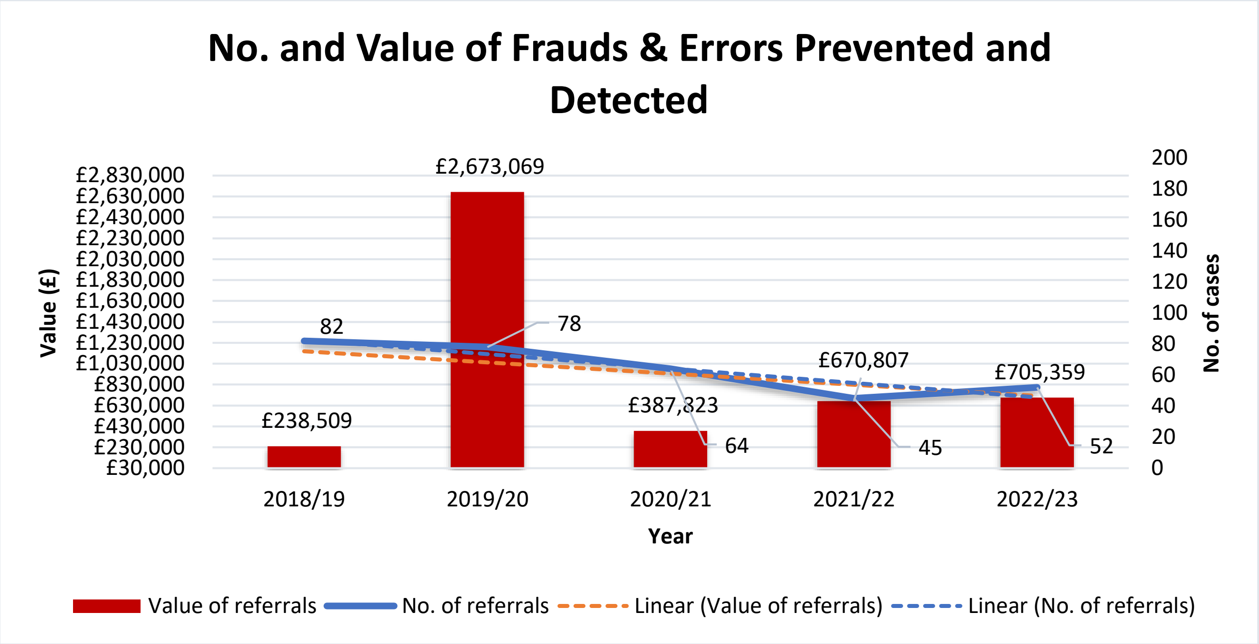
1.6. Nottinghamshire County Council participates annually in the NFI exercise and the latest data for matching was submitted in October 2022. Further details of our involvement in the NFI exercise and any reported outcomes are included in section 2.11 below.

2. Incidence of Fraud Prevention and Detection at Nottinghamshire County Council

2.1. The Council is committed to responding to the threat of fraud and it continues to take a zero-tolerance stance. This is put into practice through a broad range of activity. The continuing counter fraud strategy over the past few years has focused on prevention and detection of fraud. This can be attributed to several factors including:

- Corporate Leadership Team's and senior members' commitment to the counter fraud agenda through the development and backing of the Counter Fraud and Counter Corruption Strategy.
- Continued engagement with national research, intelligence gathering and development of data analysis.
- Risk assessment to identify emerging risks and to target reviews in higher risk areas.
- Raising awareness of the counter fraud agenda among all our staff, along with improving understanding and arrangements for capturing instances of detected and prevented fraud.
- Officers across the Council undertaking a variety of daily activities to prevent and detect fraud.
- A minority of cases result in sufficient evidence to warrant the use of the prosecution sanction.

2.2. Within this section we recognise both fraud detection and fraud prevention outcomes in assessing the value of the Council's overall exposure to suspected and possible fraudulent activity. The graph below analyses the trend over the last five years in the number and value of fraud prevention and detection cases at the Council. The dotted lines represent trends in the number and the value of cases.



2.3. The blue dotted trend line on the chart above shows an overall decline in the total number of cases compared to recent years, although numbers and values for 2022/23 are slightly higher than in 2021/22.

2.4. In 2022/23 the value of suspected fraud cases increased overall mainly due to insider fraud cases totalling £196,329 and a suspected fraudulent insurance claim for £237,526. Although the insurance claim was initially considered a potential fraud risk, this was investigated and found to be genuine, leading to no further action. Mandate frauds dropped from £527k in 2021/22 to £129k in 2022/23. Robust controls in the Business Support Centre have continued to prevent these attempts from being successful.

2.5. As indicated above, three instances of insider fraud were identified in the year, resulting in estimated losses of £196k. Instances occurred in a School, Direct Payments Team and in ICT. The cost-of-living crisis may have increased the number of employees looking for weaknesses in internal controls to manipulate. As a result of these cases, Internal Audit have carried out reviews of internal controls in those areas. Reports have been issued to management highlighting weaknesses in their processes and action plans have been agreed to make control procedures, preventative and detective measures more robust.

2.6. A summary of the cases of potential fraud and errors are identified in 2022/23 is presented in the following table.

Nature of potentially fraudulent activity and errors	No of Cases	Detection Source	Estimated Value Involved	Action Taken
Adult Social Care - internal theft of DP monies	1	Internal controls	£74,184	Reported to Police. Internal investigation and review of internal controls complete - Employee dismissed.

Nature of potentially fraudulent activity and errors	No of Cases	Detection Source	Estimated Value Involved	Action Taken
Adult Social Care – Financial Assessments deprivation of assets	16	Internal Controls	£15,470	Estimated annual reduction in NCC costs because of checks.
Adult Social Care – Direct Payments Fraud and Misuse	12	Internal Controls	4,043	Invoices raised and recovery in progress.
Adult Social Care - Staff Payment Errors	1	Internal Controls	£64,765	Internal investigation by Dept and Payroll.
Payments Team - Purchase Card fraud	6	Internal controls	£487	Monies recovered from card provider.
Payments Team - Attempt to change Supplier Bank Details (via hacked email address)	4	Internal Controls	£129,000	Suppliers were alerted to fraud attempt. Mandate changes were not made and therefore no monies were lost
ICT - Stolen New Laptops	1	Internal controls	£22,145	Internal investigation and reported to Police. Improved monitoring and checking now in place.
ICT - 3 Stolen Laptops from individuals	3	Through reports from the user	£3,225	Used devices remotely wiped and blocked. Reported to Police.
ICT - 2 Stolen Mobile Phones (assigned to staff)	2	Through reports from the user	£390	Sim blocked and loss reported to Information Governance Team and Police.
ICT - Mobile phone account hacked and procurement of multiple iPhones	1	Internal controls	£37,886	Reported to EE who notified Action Fraud. Enhanced password controls introduced.
Insurance – suspected fraudulent claims	1	Internal controls	£237,526	Internal controls. (Although fraud risk was highlighted in the early stages of the claim, eventually liability was accepted in full and the claim settled.)
School - Unauthorised overtime claims, purchase card transactions and payments	1	Internal controls	£100,000	Internal and Police investigations undertaken.
School - Purchase card	1	Internal controls	£635	Payments recovered and passwords on accounts changed.
Place Dept Household Support Grant Claims	1	Internal controls	£10,830	Payments of £9,690 stopped and further claims blocked.
Children's and Families Dept - Care Provider Claims	1	Internal controls	£4,773	Internal investigation concluded and monies recovered.
TOTALS	52		£705,359	
Blue Badge - Misuse	26	Special Enforcement days and CEO Patrols	£14,950	Misuse resulting in the issue of a PCN and cessation of passes
Disabled/Over 60's Concessions	104 Stolen 2,308 Lost	User notifications	£3,220	Cessation of passes
Cyber Security	Numerous Daily	ICT Controls	Not Quantified	External and internal defence systems to prevent or detect attacks

2.7. In compliance with the Transparency Code, NCC publishes summary information on its website each year concerning its arrangements for countering fraud. This includes the number of fraud cases investigated each year. The published details for the past three years are shown below.

Information	2020/21	2021/22	2022/23
No. employees involved in fraud investigation	29	26	40
No. professionally accredited fraud specialists	1	1	1
Estimated Cost of employee time investigating fraud	£180,607	£173,339	£205,058
No. of suspected fraud cases investigated	62	45	52

2.8. The cost of staff actively involved in identifying and preventing fraud has increased since the previous year, mainly as a result of staff time investigating internal fraud cases.

2.9. Similarly, the number of staff involved in investigations has also increased due to a wider number of staff investigating those cases. Whilst there were increased numbers of staff involved in cases, when added together, staff time spent on counter fraud work equates to just over four full time staff (including on-costs) over the year. Three of these staff work full-time in the ACFS Team.

National Fraud Initiative

2.10. The 2020-22 exercise is now complete and the key statistics for Nottinghamshire were:

28 reports matching NCC data against data from DVLA, DWP, mortality data, etc

14,209 total matches
1,551 high priority matches

NCC staff examined 14,209 matches on a risk basis

£401,777.69 outcomes identified (including £320,136 “co-estimates”)

2.11. The 2020-2022 NFI national outcomes in England (July 2022, compiled by the Cabinet Office), in the headline categories of fraud for County Councils are shown below, alongside the NCC potential fraud/error outcomes for 2020-22 and 2022-23.

Category	Cabinet Office Annual Stats (England) 2020-2022	NCC Outcomes 2020-2022	NCC 2022-2023
Pension/Payroll matches	£9.3m reported outcomes from 12,098 cases	No reported outcomes from 1,668 matches	1 case opened from 917 cases. No reported outcomes yet

Category	Cabinet Office Annual Stats (England) 2020-2022	NCC Outcomes 2020-2022	NCC 2022-2023
Trade Creditors	£6.1m detected from 955 duplicate creditor payments	£81,640 reported outcome from 7,639 matches	357 cases opened from 5,881 matches identified. No reported outcomes yet
Total Reported Outcomes	**£15.4m**	**£81,640**	**£0**
Other significant estimated results			
Blue Badges cancelled or withdrawn (no's) – based upon potential misuse	£24.4m[1] outcomes from 42,383 matches	£276,000[1] reported outcomes from 480 matches	11 cases opened from 2,193 cases. No reported outcomes yet
Concessionary Travel Passes Cancelled (no's)	£5.5m outcomes from 255,710 matches	£44,136[2] reported from 1,839 matches	All 2,641 matches processed. £56,203[2] reported outcomes from 1,815 cases
Residents Parking Permits		11 cases completed. No reported outcomes	All 12 cases opened and processed. No reported outcomes

[1] £575 per blue badge cancelled to reflect the estimated annual cost of blue badge fraud, the likelihood that badges are misused and the duration that fraudulent misuse will continue.

[2] Number of passes identified by NFI and cancelled due to person deceased, multiplied by £30.97 (£24 in 2021-22), based on the cost of reimbursement to bus operators for journeys made under the concessionary pass scheme and the duration of fraudulent pass misuse during fy 2022-23.

2.12. The 2022-23 NFI matches were returned by the Cabinet Office in January 2023, however, the majority of the checks for the matches remain outstanding. Work to investigate the matches is under way and an update on progress and outcomes will be provided in our fraud progress report in January 2024.

3. Fraud Risk Assessment

3.1. Internal Audit annually reviews and updates the Council's FRA to assess the nature of fraud and corruption threats to the Council. The assessment draws on intelligence from a variety of sources:

- National Anti-Fraud Network and National Fraud Intelligence Bureau alerts which are routinely received, reviewed and disseminated by Internal Audit.
- Liaison with the Midland Counties Counter Fraud Group – Knowledge Hub. This group is used as a forum to raise questions and share knowledge of potentially fraudulent activity or issues that have arisen at other local authorities.
- National publications, professional bodies such as CIPFA & IIA.

- Discussion with service managers across the Council to understand inherent and residual risks facing services vulnerable to fraud.
- Head of Internal Audit's knowledge and risks from core systems and the assurance mapping process.
- Analysis of incidences of suspected cases at the Council.

3.2. The latest review of the FRA, highlights the following threats as potentially having the highest impact at the Council:

External Threats

- Adult social care – personal budgets
- Adult social care – misuse of direct payments
- Adult social care – deprivation of assets to increase the Council's contribution for care costs
- Bank mandates – attempts made to make changes to supplier bank accounts
- Pension fund – continuation of payments in respect of deceased persons
- Procurement fraud – during the contract management stage of activities and including invoices for services not delivered, received or sub-standard
- Social Engineering – Phishing, vishing etc to obtain data by deception
- Blue badges – invalid use of parking permits

Internal Threats

- Payments – abuse of position and opportunity
- Collusion – two or more employees acting together to nullify internal checks
- Payroll – submission of false claims for overtime, allowances and expenses
- Procurement – abuse of procurement processes and procurement cards

4. How is Nottinghamshire County Council responding to fraud risk?

Governance and Members

4.1. The Council's Governance and Ethics Committee continues to provide the focal point for member engagement with the counter fraud agenda. Members oversee the review of policies and guidance material that underpin the delivery of the counter fraud agenda across the Council, and this continued through 2022/23:

- Counter Fraud & Corruption Policy and Fraud Response Plan
- Anti-Money Laundering Policy
- Updated self-assessment against the Fighting Fraud & Corruption Locally checklist
- Whistleblowing policy

Internal Audit and Counter Fraud

4.2. The Internal Audit Team incorporates pro-active and responsive counter-fraud work in its termly plans:

- Helping to promote a counter-fraud culture - awareness-raising articles in 'Team Talk' and 'Intranet News' over the year, and especially to coincide with the International Fraud Awareness Week in November. The online counter-fraud training was updated in October 2021 and 141 people have completed the course in financial year 2022/23.

- Detective checking – through application of its data-enabled audit strategy and use of data analytic software as part of its routine audit work.
- Prompting targeted checks by others - through the dissemination of information and advice.
- Data-matching - co-ordination of the Council's participation in ongoing NFI and NFI Recheck exercises.
- Continuous assurance – routine data monitoring for indicators of fraud in a range of corporate systems and processes.
- We have also been engaged in reviewing control procedures within the Computer Equipment Replacement Program (CERP), Direct Payment Pre-paid cards processes and auto-enhanced pay procedures for night workers.
- Counter-fraud work undertaken in relation to the household support grant, utilising data analytics and IDEA to interrogate payment records to identify duplicates and full recovery.
- Completion of actions within our Counter-Fraud Action Plan included a root-cause analysis of fraud cases. The analysis identified key priorities in relation to Direct Payment monitoring procedures, care provider claims checking and separation of duties in relation to School payments to employees and suppliers. Actions have been agreed with management in relation to these areas.
- A review of controls in relation to mandate fraud was also undertaken. A draft report has been issued to management and we have identified robust controls in place which have prevented several fraud attempts across the past few years. However, further actions are required to ensure the same level of controls are also exercised in schools.
- Outcomes in relation to ongoing fraud cases is reported to Members as part of our termly updates.

Business Services Centre (BSC)

4.3. A range of fraud preventative activities are carried out by the BSC as part of the recruitment process and the setting-up of new employees on the payroll:

- Recruitment – applying checks for new employees on the right to work in the UK, along with workflow prompts for managers to complete ongoing checks for those with temporary leave to remain in the UK. Carrying out Disclosure and Barring Service (DBS) checks (including identity checks) for prescribed categories of employee and improving reference response rates through the use of the online application. Strong controls are in place as demonstrated through the year.

The Accounts Payable (AP) Team have continued to be active in the year as part of their ongoing commitment to reduce the potential for duplicate invoice payments or fraudulent attempts to divert payments to a different bank account. They have implemented a number of activities and have others that are in progress or planned for the year including:

- AP hold a register of information relating to potential and actual fraud activities and this is shared within the Team to raise awareness, this is also reviewed at a monthly AP Controls Meeting.
- Increased collection of vendor data to ensure those who have merged or gone into administration can be checked to ensure changes can be correctly verified.
- Draft up and send out a reminder to Budget Holders about the responsibilities for ensuring appropriate checks are in place to ensure payments aren't duplicated.

- Design a basic template to send out to budget holders to request confirmation of what happened when a duplicate payment has been made (this information is normally included in email correspondence with the service).
- Issue a general reminder to all staff about Fraud Awareness and refer to e-learning modules (mandatory training), not sharing supplier bank details and making sure suppliers send invoices directly to AP instead of locally to individuals.
- Reviewing options for duplicate payment checking software and reporting. Discussions are in progress with one supplier as to the feasibility and affordability of obtaining a bespoke checking process against high value transactions. Internal Audit are also planning on further exploring inhouse options using IDEA and Excel as part of the term 2 plan.
- Review of what data is provided in response to FOI Requests to reduce the potential for fraudulent invoices to be generated.
- Mandate fraud controls – strong controls to counter attacks aimed at the accounts payable process. As demonstrated during the year this has stopped payments totalling £129k.
- Separation of duties and access to core systems – software enabled, continuous monitoring of activity in the Council's SAP accounting system to routinely detect transactions that warrant investigation. A new, annual check has been rolled out to require managers to validate continuing staff access requirements.

ICT

4.4. The cyber security agenda continues to make national headlines, and this is a primary area of focus for the ICT team including:

- Risk management process – alignment with the National Cyber Security Centre (NCSC) and Local Government Association (LGA) Directives and Best Practices.
- Digital and physical asset protection measures – these continue to successfully detect and deflect a variety of cyber related virus, malware and other malicious attacks against the Council.
- IT security standards - reviewed annually.
- Annual penetration testing by a CREST – an accredited Cyber Security Company is undertaken. Monthly stats on any successful Cyber Security incidents are collected, but so far there have been no incidents.
- External accreditation – re-certification in progress against Cyber Essentials, the Public Services Network Code of Connection (PSN) and the Data Security Protection Toolkit.
- Monthly reports on firewall blocking and SPAM email Phishing attacks.

Adult Care Financial Services Department (ACFS)

4.5. ACFS has developed a proactive approach and has in place rigorous measures to address the threat of losses due to the misuse of direct payments and intentional deprivation of assets:

- Direct Payment Policy, Agreement and staff guidance – embedded in the department's processes

- Direct Payments Auditing and ACFS escalation process – Over 80% of financial audits for 2022/23 have been completed to date and are once again identifying cases of misuse. This has resulted in prompt recovery through ongoing payments and invoices being issued for repayment where service has ceased.
- Deprivation of assets - cases continue to be identified, resulting in recovery action being undertaken in accordance with Section 70 of the Care Act 2014.

Risk & Insurance

4.6. The Risk and Insurance Team continues to take a robust approach to fraudulent claims and has a well-developed fraud protocol in place. The team continues to use a 48-point checklist to screen new claims on a risk basis to detect false, exaggerated and potentially fraudulent cases. During 2022-23 the team have completed further training hosted by Zurich Municipal focusing on how fraud risk is evolving and how it can be prevented and detected. The team have successfully defended 930 claims for compensation during the year with a savings value of £2.07m. Although one claim was identified as being potentially fraudulent in the early stages of the case upon investigation, liability was eventually accepted in full and the claim settled.

Schools Finance

4.7. The work of the Schools Finance Team makes an important contribution to the counter-fraud activities:

- Advice to schools on finance and governance - including liaison with Internal Audit in relation to potential fraud cases
- Fraud alerts – dissemination of intelligence about new and emerging fraud threats for schools through the Schools Portal
- Routine audits – audits of schools on a five-year basis incorporate checking controls designed to mitigate potential fraud risks. Findings from individual reviews provide intelligence to identify areas of fraud risk and to disseminate warnings to others.

Procurement

4.8. The Procurement Team have robust processes and due diligence in place at the tendering stage to counter fraud.

Blue Badges

4.9. Activity to identify the misuse of Blue Badges continues. The focus for counter-fraud activity in this area includes the following:

- Issue of Penalty Charge Notices (PCNs) where Enforcement Teams identify incorrect use of badges.
- Vigilance in identifying suspicious applications for badges, including repeated claims of badges being lost.
- Liaison with the City Council and Police Compliance and Fraud Officer to share intelligence of badge misuse.
- Participation in the NFI to identify and cancel active badges linked to deceased badge holders.

In addition, in 2022-23 three specific enforcement days were carried out as the team tightened up on enforcement. These were centred mainly around the Forest ground, due to an increase in Blue Badge parking adjacent to the ground. Two instances of misuse were picked up within the 49 checks undertaken. In total, 24 Blue Badges have been seized in the year and 11 PCNs have been issued for blue badge misuse. All seizures have been done during a Civil Enforcement Officer's day-to-day patrol.

Concessionary Passes

4.10 Key actions to counter the fraudulent use of concessionary travel passes centre around failure to notify the Council of the death of a pass holder:

- Participation in the bi-annual NFI process
- Linking in with the Council's 'Tell Us Once' process to facilitate notification of the death of a pass holder and establishing closer links with the Registration Service appears to have reduced the number of NFI matches significantly.
- The hot-listing system designed to facilitate remote cancellation of any badges that should no longer be in use, has been delayed due to technical issues but is starting in July 2023. The facility for prompt cancellation of badges will most likely prevent some instances of fraud.
- We have now identified a national website where we can filter Nottinghamshire deaths weekly and check against our database. This has enabled deceased pass holders to be quickly identified and should reduce the number of NFI matches moving forwards.

5. Counter Fraud Priorities for 2023/24

5.1. The following sets out priorities for 2023/24, all of which will be led by Internal Audit.

Action	Timescale
Pro-active work with the Travel & Transport team to respond to the threat of Blue Badge and Concessionary Travel Fraud, including an audit of the notification process (Tell Us Once) and the hot-listing system once established.	November 2023 (Term 2 Plan)
Continue to work with the Business Service Centre to develop additional in-house options to identify duplicate payments using Excel and IDEA Audit software, in line with key actions identified above.	November 2023 (Term 2 Plan)
Continue to review progress with actions from the FFCL self-assessment and address outstanding actions.	Ongoing to March 2024
New risk areas for consideration in the 2023-24 plan:	
The audit of mandate fraud has highlighted the need to work with School's Finance to raise awareness in Schools of the risks of mandate fraud and the best practice needed to prevent loses.	September 2023
Working with Pensions and Blue Badge teams to consider sources of data to facilitate the early detection of deceased notification so that pensions payments and blue badges can be cancelled much more promptly.	September 2023
Review fraud risk assessment and update to include emerging fraud risks.	September 2023
Insider Fraud – As part of International Fraud Awareness Week 2023 – raise awareness of insider fraud threats and the need for robust internal controls. Promote fraud awareness training and access to staff welfare and support programmes for those who may be struggling.	November 2023