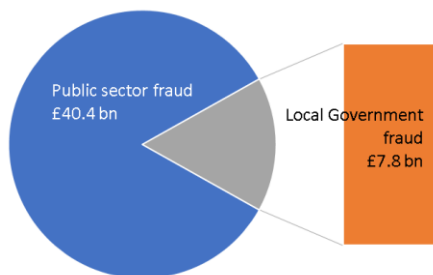


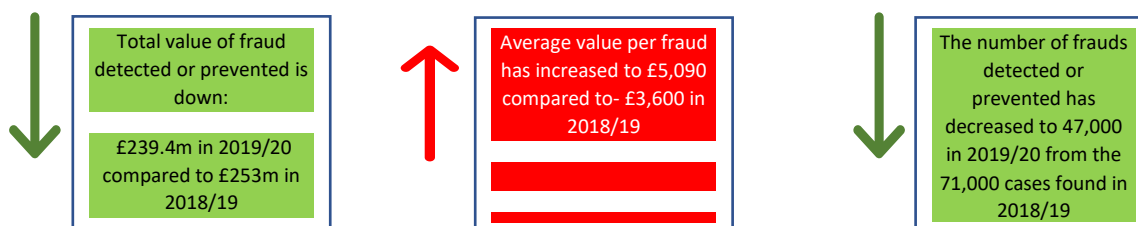
ANNUAL FRAUD REPORT 2021/22

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. Its fraud indicator estimates were most recently refreshed in 2017, and these suggest significant losses to fraud for local government and the public sector more widely.



- 1.2. Whilst the above estimates have not been updated since 2017, recent trends suggests that tougher approaches to tackling cross-boundary and organised fraud and corruption attempts, as well as addressing new risks such as social care fraud and cyber issues are necessary. Local authorities have set up various working groups to look at fraud risks including the area of social care fraud and how this might be tackled. The Midland Counties Counter-Fraud Group, who we are a member of, will feedback on any developments.
- 1.3. The key fraud risk areas for local government are highlighted by the CIPFA Counter Fraud Centre (CCFC)'s annual 'Counter Fraud and Corruption Tracker' (CFaCT). The Council participates in this annually, however, the exercise was not undertaken in 2020/21. The Annual Fraud Survey was suspended last year and is being operationally reviewed to cover relevant fraud and is likely to be reinstated in the near future. The latest update from August 2020 however, reported the following key findings on the incidence of fraud across local government.

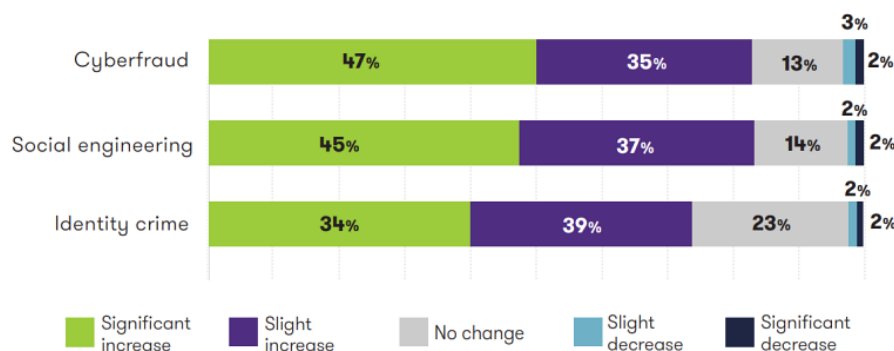


The main targets for fraud and national trends in incidence may be broken down as follows:

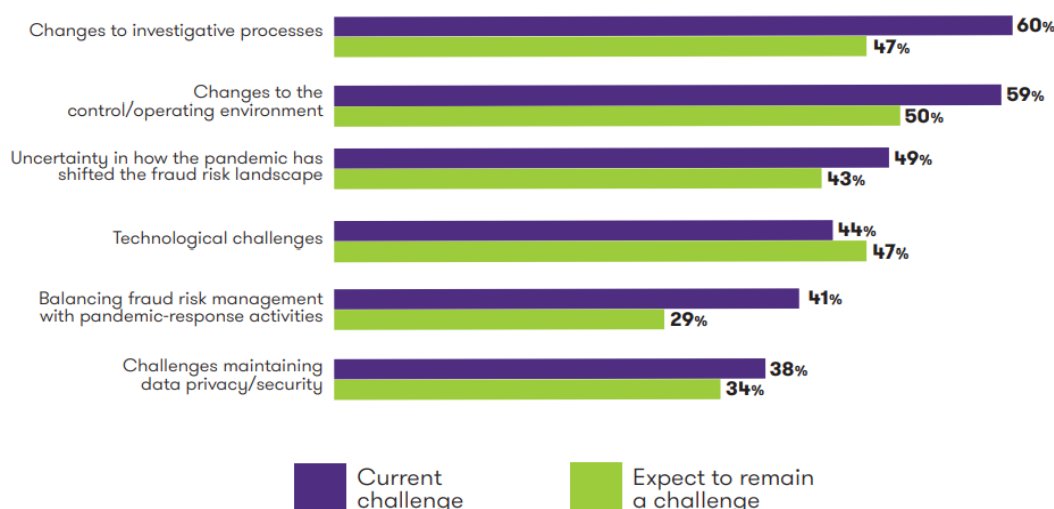
Target	Trend (volume)	Target	Trend (volume)
Disabled parking concessions	UP	Serious & Organised Crime	Down
Adult Social Care – personal budget	UP	Payroll	Down
Adult Social Care - other	Down	Expenses	UP
Insurance	UP	Recruitment	Down
Procurement	Down	Pension	Down
Mandate Fraud	UP		

Source: CFaCT Summary Report 2020 – based upon estimated total figures

- 1.4. In light of the lack of more recent data, we have identified a report produced by the Association of Certified Fraud Examiners (ACFE) and Grant Thornton and this indicates that many organisations have continued to uncover more fraud since the onset of the pandemic. Furthermore, there is an expected change in the specific fraud risks over the 12 months from June 2021 as follows:



- 1.5. In addition, the findings indicate the top challenges facing anti-fraud include the following changes:



- 1.6. The above threats have been considered as part of our fraud risk assessment (FRA) outlined in section 3 and we have considered them in our programme of work for 2022/23.

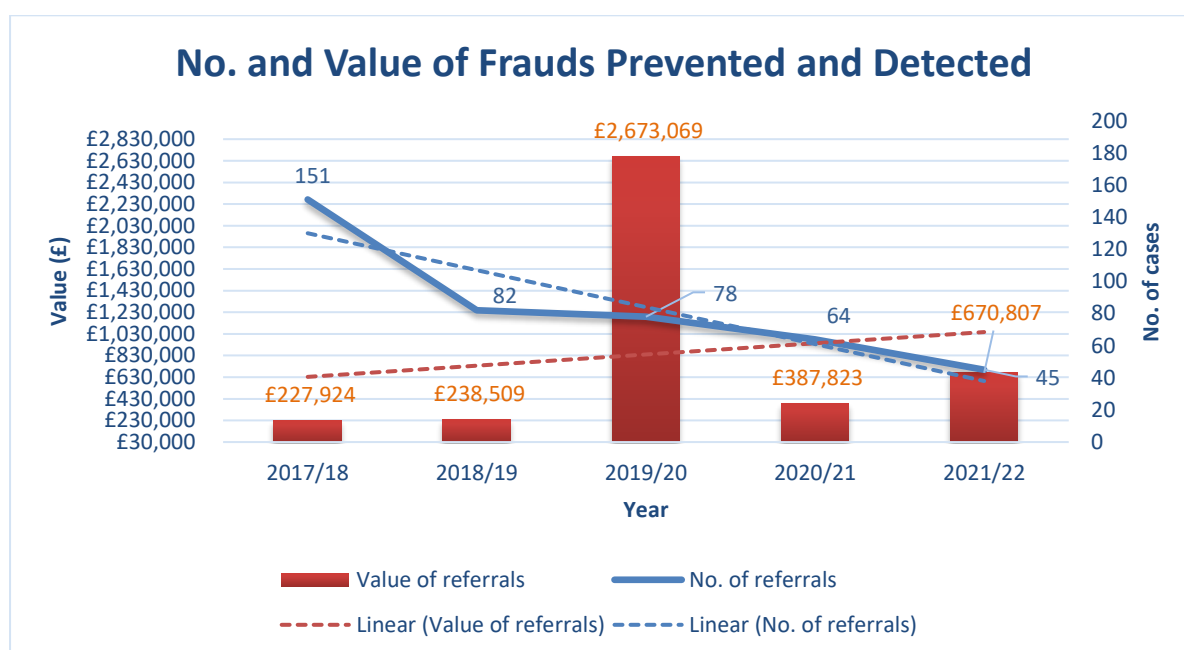
2. Incidence of Fraud Prevention and Detection at Nottinghamshire County Council

- 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 undertake 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. In line with the CFACT Summary Report 2020, the blue dotted trend line on the chart above shows a steady decline in the total number of cases compared to recent years.

2.4. In 2021/22 the value of frauds prevented increased due to two unsuccessful attempts to have fraudulent payment requests processed, totalling £527,040. Both attempts were blocked by Business Support Centre controls, and controls have been enhanced since these attempts were made. Further work is planned in 2022/23 in this area as this is seen to be a growing threat.

2.5. A summary of the cases of potential fraud identified in 2021/22 is presented in the following table.

Nature of potentially fraudulent activity	No of Cases	Detection Source	Value Involved	Nature of Activity
Adults Social Care – Financial Assessments – deprivation of assets to avoid paying own care costs	26	Internal Controls through ASCH Reviewing Team	£116,396	People were charged the full costs of the service, saving the Council on Social Care costs

Nature of potentially fraudulent activity	No of Cases	Detection Source	Value Involved	Nature of Activity
Adults Social Care – Direct Payments Fraud and Misuse	11	Internal Controls – ACFS Annual Audits	£8,120	Recovered through ongoing payments
Adults Social Care – Ceased Direct Payments Misuse	1	Internal Controls – ACFS Annual Audits	£15,675	Invoice raised and recovery in progress
Pre-paid Financial Services Card – Cyber Crime	3	Information Sharing – Fraud network	£0	Losses prevented - compromised cards cancelled due to early intervention
Adult Social Care – Excessive Care Home provider claims	1	Internal Checking Controls	£2,000	Monies recovered
Adult Social Care – Deprivation of Assets - Theft from service user by family member	1	Internal Checking and Police Notification	£1,576	Invoice raised for recovery of care payment. Police prosecution for family member pending
Mandate Fraud	2	Internal Checking Controls	£527,040	Attempted change of bank details – detected and prevented
TOTALS	45		£670,807	
Blue Badge – Misuse	19 stolen 268 lost badges cancelled	Civil Parking Enforcement Officers	£10,925 ¹	Misuse resulting in the cessation of pass
Disabled/Over 60's Concessions	82 stolen 1882 Lost		£1,968 ²	Lost or stolen badges are not necessarily used fraudulently
Cyber Security	numerous daily attempts	ICT controls	Not quantified	External and internal defence systems to prevent and detect attacks

- 2.6. 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	2019/20	2020/21	2021/22
No. employees involved in fraud investigation	29	29	26
No. professionally accredited fraud specialists	1	1	1
Estimated Cost of employee time investigating fraud	£159,167	£180,607	£173,339
No. fraud cases investigated	81	62	45

¹ Based upon NFI theoretical estimates of prevented fraudulent use being £575 per blue pass

² Based upon NFI theoretical estimates of prevented fraudulent use being £24 per concessionary pass

- 2.7. The cost of staff actively involved in identifying and preventing fraud has decreased since the previous year, partly due to the National Fraud Initiative (NFI) exercise taking place bi-annually and partly due to other work pressures and recovery from Covid-19 taking priority.

National Fraud Initiative

- 2.8. The 2020-22 exercise is still in progress, however, the key statistics for Nottinghamshire for the 2018-20 exercise were:



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



14,121 total matches
1,551 high priority matches



NCC staff examined 8,026 matches on a risk basis and 1 case remains in progress



£64,154 of outcomes identified

- 2.9. The 2018-20 NFI national outcomes (July 2020, compiled by the Cabinet Office), in the headline categories of fraud for County Councils are shown below, alongside the NCC potential fraud/error outcomes.

Category	NFI 2018-20	NCC 2018-20	NCC 2020-22
Pension Overpayments (Deceased)	£55.5m	£83,028	No outcomes yet to report. 542 from 1557 (35%) matches checked to date
Personal budgets	£2.1m	£2,049	Not included in the latest matching exercise due to NFI GDPR issues
Trade Creditors	£5.1m	£0	£81,640
Payments to Private Care Homes for Deceased Persons	£5.1m	£6,409	Not included in the latest matching exercise due to NFI GDPR issues
Total	£67.8m	£91,486	£81,640
Other significant estimated results			
Blue Badges cancelled or withdrawn (no's)	46,750	576 cases	479 cases – with a potential value of £275,425
Concessionary Travel Passes Cancelled (no's)	151,815	115 cases	1,839 cases with a potential value of £44,136
Theoretical estimates based on average value of cases above (not previously estimated in this way before) – see footnotes 1&2.		691 cases	£319,561

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

- Bank mandates – attempts made to make changes to supplier bank accounts
- Pension fund – continuation of payments in respect of deceased persons
- Blue badges – invalid use of parking permits
- 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
- 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

Internal Threats

- 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
- Payments – abuse of position and opportunity

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 2021/22:

- Counter Fraud & Corruption Policy and Fraud Response Plan
- Anti-Money Laundering Policy
- 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. Since the relaunch of online counter-fraud training amongst Council staff in October 2021, 299 people have completed the course.
- 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 and data-washing – co-ordination of the Council's participation in ongoing NFI and NFI Recheck exercises, along with engagement with the national Government Agency Intelligence Network (GAIN) to check for any links with known serious and organised crime. Results of the latest exercise in May 2022 have come back without any concerns in relation to organised crime and the benefit of further checks will be considered.
- Continuous assurance – routine data monitoring for indicators of fraud in a range of corporate systems and processes.

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.
- Mandate fraud controls – strong controls to counter attacks aimed at the accounts payable process. As demonstrated during the year this has stopped two payments totalling £527,040. It is a concern that these are examples where fraudsters have infiltrated vendor systems to attempt to change bank details. Whilst the Council's controls remain resilient to these threats, in the last financial year approximately 250 bank account amendments have been made in BMS for various vendors and because of these attempts, the Council's controls have been enhanced. Further work is also planned to review third party controls and raise awareness to suppliers of these risks.
- 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:
- 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 policies - reviewed annually
 - External accreditation – in-progress - re-certification against Cyber Essentials, the Public Services Network Code of Connection and the Data Security Protection Toolkit.

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 – now resumed following the diversion of resources to deal with the pandemic emergency. Over 80% of financial audits for 2021/22 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 use a 48-point checklist to screen claims on a risk basis to detect false, exaggerated and potentially fraudulent cases. During 2021-22 the team completed the Council's own Fraud Awareness Training. In addition, key officers within the team also took part in a virtual refresher training session hosted by Zurich Municipal which focused on the risk of fraudulent personal injury claims resulting from slips and trips. Although no fraudulent claims were identified, 855 claims were successfully defended during the year with a savings value of £2.5m.

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 where Enforcement Teams identify incorrect use of badges - NCC has lobbied Central Government to consider making enforcing Blue Badge fraud simpler
- 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.

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
- Rolling out a hot-listing system which will enable remote cancellation of any badges that should no longer be in use in 2022.

5. Counter Fraud Priorities for 2022/23

5.1. The following sets out priorities for 2022/23, 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.	March 2023
Review progress with actions from the FFCL self-assessment and address outstanding actions.	Reviewed November 2021 and continues to March 2023
The Business Service Centre to work with Internal Audit to develop additional in-house options to identify duplicate payments using Excel and IDEA Audit software.	September 2022
A piece of work is currently underway to complete a root-case analysis of past fraud cases and identify any key control risks to enhance further learning.	September 2022
Review internal and external controls in relation to preventing mandate fraud.	March 2023