Appendix 1

Counter Fraud – Annual Report 2020/21

1. Introduction

This is the second annual Counter Fraud Report. It provides details on all the counter fraud activities undertaken within the Council in the 2020/21 financial year.

The annual report covers:

- The National Fraud Initiative - 2020/21
- The work of the Council's Counter Fraud Team over the year
- The Council's approach to fraud risk in Covid Grants
- Details of any reports made under the Money Laundering, Terrorist Financing and Transfer of Funds (Information on the Payer) Regulations 2017 (MLR 2017)
- Details of any reports made in respect of the Bribery Act 2010
- Items raised under Whistleblowing (the Public Interest Disclosure Act 1998)
- Applications made under the Regulation of Investigatory Powers Act 2000

2. National Fraud Initiative (NFI) – 2020/21 Exercise

In October 2020, the Council submitted data to the Cabinet Office as part of the 2020/21 National Fraud Initiative (NFI) exercise. The table below shows progress on the matches:

Table 1 2020/21 Exercise

Total Number of Matches	Number of High Risk Matches	Number of Matches Closed as at 6th July 2021	Number of Matches in Progress as at 6th July 2021	Number of matches identifying a Fraud (exc Rechecks)	Number of Matches identifying an error	Financial Outcome (exc Rechecks)
4,873	676	1,254	79	4	73	£11,068

To date, the NFI exercise has identified the following errors and frauds:

- 96 Blue Badges have been cancelled as a result of comparing Council records to the Department of Work and Pensions deceased data (71 of these are included in the Error figure in the table above). Although there is no direct financial saving to the Council, the Cabinet Office estimate that this will save £55,200 to reflect lost parking and congestion charge revenue (based on a standard national saving of £575 per badge).

- Benefit had been paid in error to a deceased individual for 9 weeks. £884 is currently under recovery.

- 1 residents parking permit was cancelled as a result of comparison to Benefits Agency deceased data.

- 3 individuals had failed to declare their student loans when claiming housing benefit (£10,184 was under recovery).

- 1 residents parking permit had been obtained fraudulently and has been cancelled.

3. Counter Fraud Team

The Counter Fraud Team consisting of 3FTE, which increased to 4.4FTE by Feb 21 and based within Revenues, Benefits and Exchequer Services have focused on:

- Delivering the Covid-19 Business Support Grant scheme
- Raising fraud awareness
- Preventing fraud
- Detecting fraud
- Understanding emerging fraud risks

<u>Raising Fraud Awareness</u>

The highlights for this stream include;

- Fraud awareness training for staff.
- Ensuring Alerts are communicated.

Preventing Fraud

The highlights for this stream include;

Continuing to provide additional checks for Right to Buy cases

(a) Continuing to work with Adult Social Care to prevent fraud in supported accommodation.
(b) Working with Derby Homes to undertake pro-active checks to prevent and detect fraud.
(c) Continuing to host the East Midlands Fraud Group with local partners and agencies to share best practice and identify emerging fraud risks.
(d) Continuing to work with Derbyshire Police following identification of a case involving potential money laundering.
(e) Undertaking pre-payment and fraud checks to support Covid-19 Business Grant awards.

Detecting and Investigating Fraud

The highlights for this stream include;

(a) 7 Derby Homes properties recovered (e.g. illegal sub-letting, breach of tenancy) and 5 Housing applications withdrawn.
(b) £744,082.03 savings delivered, consisting of £195,109.71 cashable savings and £548,972.32 value for money savings. Value for money (VFM) savings includes preventing unnecessary expenditure and loss of future income (Table 2).
(c) Continuing to provide intelligence to support Modern Slavery and Organised Crime Groups and to support the Rogue Landlord Initiative.
(d) Working with the Council's Financial Investigator to maximise income where appropriate.
(e) Continuing to participate in the Council Tax Single Person Discount Review which commenced in September 2019.
(f) The team has played a significant role in the Covid-19 Business Support Grant scheme providing operational support, pre-payment and post payment fraud checks, data-matching and development of the post payment assurance plan.

Understanding Emerging Fraud Risks

In addition to investigating fraud the team is working with the following service areas to minimise their exposure to fraud risks;

(a) Social care and direct payments.
(b) Homeless team/RTB team.
(c) Housing Benefits – specifically Supported Accommodation where enhanced rates of Housing Benefit can be claimed.
(d) Revenue & Economic regeneration – providing pre-payment assurance and fraud checks to support the Covid-19 discretionary Business Support scheme.

The overall savings breakdown for the team in the 2020/21 financial year is shown in Table 2 below.

Table 2 - Counter Fraud Team Savings Breakdown 2020/21

Description	Number	VFM Saving* £	Actual Saving/Income £
Council Tax/ NNDR			
Council Tax single person discounts removed Non NFI NNDR	 78 3	 **49,121.62**	 **39,261.95** **22,476.14**
Local Council Tax Support	11	**4159.68** (Weekly amount x21)	**11,216.00**
General change in liability	41		**71,316.86**
Housing Benefit			
Housing Benefit cancelled / reduced	12	**15,931.02** (Weekly amount x 21)	**45,588.76**
Housing			
Illegal succession, sublet, breach of tenancy	7	(7 x £46,500) 325,500.00	
Housing Application stopped	5	**16,400**	
Right to Buy	2	**137,860.00** (Value of RTB discount)	
Civil Penalties	75		**5250.00**
TOTAL	**234**	**548,972.32**	**195,109.71**

*VFM savings based on guidelines for calculating value associated with fraud according to the Cabinet Office calculations.

** The Cabinet Office calculates tenancy fraud at £93k per property recovered based on a four-year average fraud indicated by previous results. Results at Derby indicate the average length of fraud to be two years therefore we have used a prudent value of £46,500 per property recovered.

4 **Covid Grants – Fraud Risk**

When the Government announced its support grants for businesses affected by the Covid-19 Pandemic in April 2020, the Head of Revenues, Benefits & Exchequer Services was tasked with leading on the Council's administration of the grants. The Head of Revenues, Benefits & Exchequer Services made the early call that the Council needed to minimise the risk of fraud and error in the system that was being developed to administer and pay these grants. He worked closely with the Head of Internal Audit and the Council's Senior Counter Fraud Investigator to establish processes that would proactively seek to prevent and detect fraud entering the system. When the Local Authority Discretionary (or "Top-Up") Grant Fund and Additional Restrictions Grant (ARG) schemes were introduced, a similar approach was adopted by the Economic Growth team led by the Senior Derby Enterprise Growth Fund Manager.

Role of Counter Fraud Team

The Counter Fraud Team have played a substantial role in the Business Support Grant process and continue to do so. Tasks undertaken are:

- Assisted with development of application forms for various grant schemes and testing.
- Devised a robust risk assessment plan.
- Undertook 'Spotlight' checks on all limited companies and analysed responses (Spotlight is a government automated tool providing due diligence checks).
- Undertook Experian checks through NFI and analysed responses.
- Manually provided due diligence checks on appropriate cases utilising available intelligence held by the authority, via open source and other legal gateways.
- Liaised with other authorities where necessary to prevent cross border fraud.
- Liaised with the National Anti-Fraud Network on cases of potential organised fraud.
- Investigated grant applications where necessary.
- Reviewed documentation submitted to identify manipulated or false items.
- Provided a Single Point of Contact for fraud checks and referrals.
- Post payment checks including National Fraud Initiative data-matching.
- Claw back of funds as required.

The Covid-19 Business Support Grant programme has introduced numerous grant schemes to support businesses during periods of local and national restrictions since March 2020 to date.

The Government require grant awards to be paid within a specific timeframe. This has required working at pace to deliver the various schemes and continually adapt processes and checks depending on the eligibility criteria of the different grants available.

Post payment checks to date have shown that the comprehensive regime of pre-payment checks undertaken by the authority have provided a robust framework which has minimised exposure to fraud.

Role of Internal Audit

As well as an advisory role on mitigating fraud risk, Internal Audit's key role was to provide forensic, data interrogation and data analytics support throughout the process. This involved:

- Data matching and analysis to identify 'duplicate applications', based on business name, contact information, bank account fields etc, which aimed to reduce the likelihood of duplicate or inappropriate payments.
- Analysing applications 'cleared for payment' for particular grant schemes to highlight instances whereby the business had already been granted financial support from one of the other schemes. This was to prevent the likelihood of duplicate payments, incorrect applications, and also stopped payments being made from the wrong schemes.
- Identifying instances across the business support schemes, where different businesses had specified the same bank account numbers and sort-codes, or the same contact information, which helped identify possible fraudulent efforts for further investigation.
- Identifying applications relating to businesses that had been automatically authorised for 'top up' payments for a specific scheme, but that had 're-applied' when not required to do so. This again helped reduce the likelihood of duplicate or incorrect payments to businesses.
- Identifying potential suspect applications submitted at strange times (e.g. between midnight at 4am), often in 'batches' where applications shared similar characteristics such as the email domain. This again highlighted suspect applications for further investigation before payment was authorised.
- Identifying applications for different businesses which had been submitted from the same IP addresses, and applications for different businesses submitted from the exact same smartphone model, browser version and operating system level, which may identify suspect activity and possible attempted fraud.
- Using data analytics to highlight examples whereby the geo-location of applications for Derby businesses were submitted from outside the City, e.g. London, which may again be a sign of suspect activity and flagged to management for further investigation.
- Performing a 'sort-code analysis' of applications already flagged for fraud and audit investigation, where Derby businesses were specifying "High Street branches" based in locations outside of the City.
- Undertaking regular data matching to NAFN (National Anti-Fraud Network) intelligence bulletins, to check applications made to Derby City Council do not match the bank accounts and contact information for known frauds targeting the grant schemes across the UK. This highlighted some instances where payment was made or had been 'authorised for payment'.

Through doing these fraud and error checks, Internal Audit was also able to highlight examples of general data quality issues back to the processing teams to ensure erroneous or incomplete data would not impact the processing of claims and payment. Audit has also provided management with advice on security concerns associated with the permissions which demonstrated a failing to protect the grant application data stored on the Council's file server, which could result in unauthorised access to financially sensitive information and/or amendment of records thereby increasing the risk for fraud and/or 're-direction' of payments.

In general, the data sent through to audit was analysed and returned to the teams on the same day to help ensure they had timely results on which to base their funding decisions, and to avoid delay to those eligible businesses requiring financial support.

5 Public Interest Disclosure Act 1998

There were 5 disclosures made under the Council's Whistleblowing policy in 2020/21.

Table 3 : Whistleblowing Disclosures 2020/21

Case Number	Description	Progress/Outcome
21/1	Potential false mileage claims at a LEA school.	Control improvements suggested to school
21/2	Issues connected to the Council's Grievance policy	Based on independent assessment as part of the Appeals process by the Strategic Director, it was concluded that the process had followed the Council's Grievance Policy. The Audit review has identified a number of areas of the policy that would benefit from further clarification/ improvement.
21/3	Failure to follow Council's policies and procedures - grievance/disciplinary	As above (21/2)
21/4	Failure to follow the Council's policies and procedures – Appeal and Grievance	As above (21/2)
21/5	Incident involving member of staff in a Council residential establishment – potential Safeguarding issue.	Referred to the LADO who deemed it to be below safeguarding threshold. Investigation carried out by Deputy Head of Service. Several areas of practice needing priority development.

6 The Money Laundering, Terrorist Financing and Transfer of Funds (Information on the Payer) Regulations 2017 (MLR 2017)

There were no reports of potential Money Laundering made under the Council's Anti-Money Laundering Policy in 2020/21.

7 Bribery Act 2010

There were no reports of suspicions of bribery made under the Council's Anti-Bribery Policy in 2020/21.

8 Regulation of Investigatory Powers Act 2000

The Council is wholly responsible for the administration and recording of Part II RIPA activity (covert surveillance and the use of covert human intelligence sources). Part I activity (access to communications data) is undertaken, on behalf of all local authorities, by the National Anti-Fraud Network (NAFN). As part of the statutory framework within which those powers are exercised, the Investigatory Powers Commissioners Office (IPCO) requires each regulatory authority that undertakes surveillance activity to put in place governance arrangements that provide decision makers with oversight in respect of the use of surveillance tactics within the authority specifically, in relation to numbers, type and the integrity of the records system.

The Council is obliged to maintain a central record of all applications made using the RIPA procedures regardless of whether they have been authorised or refused by either of its Authorising/Designated Officers, the National Anti-Fraud Network (NAFN) (in respect of communications data applications) and/or the local magistrates' court.

The authorisation, review, renewal/extension and cancellation of covert surveillance requests are recorded in the Council's central register of authorisations. The central record is maintained by Legal Services.

During the 2020/21 administrative year, there were no applications made for either directed surveillance or the use of covert human intelligence sources (CHIS) under Part II of RIPA.