COUNTER FRAUD FRAMEWORK REPORT

29 September 2022

ANNEX 1

Middlesbrough moving forward

Assistant Director - Corporate Fraud: Jonathan Dodsworth

Head of Internal Audit: Max Thomas

Veritau

INTRODUCTION

1 Fraud is a significant risk to the UK public sector. Losses to local government due to fraud results in less funding for public services. The government estimates that the taxpayer loses up to £51.8 billion to fraud and error in public spending every year and 40% of all crime committed in the UK is categorised as fraud[1].

2 To effectively combat fraud the Council needs to have a counter fraud framework that helps it prevent, detect and deter fraud. Counter fraud work needs to develop at least as quickly as the techniques used by fraudsters.

NATIONAL PICTURE

3 The Institute for Fiscal Studies reports that the UK is experiencing a "cost of living crisis"[2] as a result of a number of financial factors. The insurance company Zurich reports a "sharp increase in insurance fraud as cost of living pressures contribute to a rise in bogus claims"[3]. Fraud is expected to become more prevalent during this period and councils may see an increase in false claims for discounts and benefits. The public will also be targeted. There have been reports of scam telephone calls and text messages made to members of the public purporting to offer financial support (eg government support for energy bills) but are in fact attempts to use the current situation as a way to defraud people.

4 The Public Sector Fraud Authority (PSFA) was launched in August 2022. The organisation seeks to modernise the government's counter fraud response. The PSFA aims to produce £180 million in fraud benefits in its first 12 months. It will agree counter fraud plans with, and provide support to, central government departments and other public bodies to help combat fraud. The PSFA will focus on ministerial bodies but will share best practice and standards with local government[4].

5 Cybersecurity continues to be an area of focus for the public and private sectors as organisations rely more on online resources to deliver services and facilitate productivity (eg homeworking). In a recent report RSM UK expressed concern that when an organisation's infrastructure extends into the homes of staff that this presents an easier target for criminals. A survey that formed part of the report found the number of medium sized business owners reporting successful cyber attacks had increased by 35% compared to the previous year[5].

6 The World Economic Forum's 2022 Global Risk Report states that 95% of cybersecurity issues stem from human error[6]. Luton Council was subject

[1] Fraud and Error (Ninth Report of Session 2021/22), Public Accounts Committee, June 2021, HM Government
[2] Response to Government Cost of Living Statement, Institute for Fiscal Studies, May 2022
[3] Cost of Living Press Release, Zurich Insurance Group, July 2022
[4] Public Sector Fraud Authority Mandate, HM Government, September 2022
[5] The Real Economy - Cyber Security report, RSM UK, April 2022
[6] Global Risks Report 2022, World Economic Forum, January 2022

to a payment diversion fraud (also known as mandate fraud) perpetrated by organised criminals. A compromised user account was used to request a change of bank account, resulting in the diversion of a £1.1m payment. To date this has not been recovered. This highlights the importance of strong controls and regular messages to employees to raise awareness of fraud.

LOCAL PICTURE

7 Officers in service departments play a key role in ensuring controls operate correctly to help prevent fraud and raising suspicions of fraud with the counter fraud team when they occur. Over the last two years, the counter fraud team has been working to develop closer relationships with departments across the council, in areas where fraud is a higher risk. This has resulted in a steady increase in the number of requests for assistance and referrals of fraud. The team will continue to develop these relationships further over the coming year and will be targeting a number of new areas including children's social care and insurance.

8 The vast majority of fraud reported comes from members of staff as opposed to residents. Further work is planned to promote the counter fraud hotline to the public.

9 The National Fraud Initiative (NFI) is a data matching exercise run every two years by the Cabinet Office. Councils and other public bodies are required to provide a range of data sets which are matched together to produce data matches for individual organisations to review and investigate. Substantial numbers of these matches are produced for Middlesbrough Council – the 2020/21 exercise produced 5,800 matches. Workload and resourcing issues across a number of service areas led to only a small number of matches being reviewed. The counter fraud team will offer support to service areas to help review matches produced in the upcoming 2022/23 exercise.

COUNTER FRAUD FRAMEWORK

10 The Council has a robust counter fraud framework which includes a counter fraud strategy and associated action plan, an anti-fraud and corruption policy, a fraud risk assessment, and a number of related policies (eg whistleblowing). A review of the framework is conducted annually.

11 The Council's current counter fraud and corruption strategy was adopted in 2020. The strategy sets out the Council's aims for counter fraud work over the next few years. The strategy also includes actions needed to maintain and develop counter fraud arrangements at the Council. The associated strategy action plan is reviewed and updated annually. This year's update is contained in appendix A. It details progress made against last year's plan and introduces new priorities for the counter fraud team in 2022/23 taking into account local and national developments.

New objectives this year include:

- monitoring and implementing guidance from the newly formed Public Sector Fraud Authority
- promoting counter fraud work to new service areas at the Council
- increasing responsibility for the evaluation and investigation of National Fraud Initiative data matches.

12 The current review identified that the Anti-Fraud, Corruption, and Bribery Policy requires updating due to the Police, Crime, Sentencing and Courts Act 2022. The covering report contains details of the changes required and the revised policy is in Annex 2.

FRAUD RISK ASSESSMENT

13 It is recognised good practice for councils to assess their risk of fraud on a regular basis. An updated fraud risk assessment is contained in appendix B.

14 The risk assessment highlights areas of work to be undertaken by the internal audit and counter fraud teams (eg fraud awareness training) in addition to actions included in the counter fraud and corruption strategy action plan.

15 The current review downgrades Covid-19 grant related fraud to a low risk level. The Council is not currently distributing any new Covid-19 related grants and considerable work has been undertaken to prevent fraud from occurring throughout the pandemic. The risk level of fraudulent insurance claims has been upgraded following reports of increased false claims from the Zurich Insurance Group.

APPENDIX A: COUNTER FRAUD STRATEGY ACTION PLAN

Veritau have responsibility for maintaining, reviewing, and strengthening counter fraud arrangements at the Council. This includes an annual review of the Council's counter fraud strategy action plan.

Veritau also provide a number of other ongoing activities including:

- a rolling programme of fraud awareness training for officers based on priorities identified through the fraud risk assessment and any emerging issues
- annual campaigns to promote key issues, including cyber security, fraud awareness, anti-bribery and money laundering, and whistleblowing
- regular reporting of counter fraud activity to the Corporate Affairs & Audit Committee.

New one off and developmental activity:

Ref	Action Required	Target Date	Responsibility	Notes
1	Review guidance issued by the Public Sector Fraud Authority (PSFA); identify recommended actions and implement as required.	September 2023	Veritau	The newly formed PSFA is expected to develop their offering to the public sector over the next year.
2	Promote counter fraud work to more departments at the Council.	March 2023	Veritau	Explore undertaking counter fraud work with council departments where work is not currently ongoing, eg Children's Social Care and Insurance.
3	Increase responsibilities around the investigation of National Fraud Initiative data matching.	March 2023	Veritau	The counter fraud team currently administer the National Fraud Initiative but do not review the matches produced. Veritau will offer support to review upcoming matches in a number of service areas.

Ref	Action Required	Target Date	Responsibility	Notes
4	Update the Council's Anti-Fraud, Bribery and Corruption Policy.	September 2022	Veritau	The Fraud and Corruption Prosecution Policy requires updating to reflect changes to cautions introduced by the Police, Crime, Sentencing and Courts Act 2022.
5	Promote counter fraud reporting lines to members of the public and staff.	March 2023 (was 2022)	Veritau / Communications Team	This objective is carried over from the previous year. Further work is required to promote fraud reporting internally and externally.

Completed activities:

Ref	Action Required	Responsibility	Update
1	Raise awareness of cyber security issues and promote good practice.	Veritau / Communications Team	Working with council officers Veritau ran an anti-cybercrime campaign in October 2021 to mark cyber security awareness month. The campaign will be repeated and form part of Veritau's annual awareness raising activity.
2	Promote the Council's counter fraud policy framework.	Veritau / Communications Team	The Council's anti-bribery and anti-money laundering policies were highlighted to staff on world anti-corruption day in December. The whistleblowing policy was raised during world whistleblowers' day in June. Awareness raising activity for these policies will continue on an annual basis.
3	Explore additional verification tools for social care financial assessment process.	Veritau / Adult Social Care Services	New tools to help verify applications for social care are now in use by financial assessment officers.

Ref	Action Required	Responsibility	Update
4	Increase sharing of counter fraud intelligence to enhance fraud prevention.	Veritau	Intelligence sharing processes are now in place to quickly alert council officers of fraud issues raised regionally and nationally.

APPENDIX B: Fraud Risk Assessment (September 2022)

Risk Area	Risk Description	Risk Controls	Risk Category	Risk Mitigation
Adult and Children's Social Care Fraud	For adult social care, losses can occur through deprivation or non-declaration of capital which can involve the transfer or disguise of property in order to avoid paying for residential or domestic care provision. Residential homes could also continue to claim for customers who are no longer in residence (eg after they pass away). In both adult and children's social care, fraud can occur through the misuse of the Direct Payment scheme. For example, where monies allocated to meet a customer's assessed needs are not used to procure support services.	Applications for care funding are carefully assessed to ensure that recipients meet the eligibility criteria and that any financial contribution for care by the customer is correctly calculated. A range of monitoring and verification controls are operated by the Council. This includes requiring customers in receipt of Direct Payments to have a separate bank account for managing these funds and complying with monitoring procedures to verify spending. In instances of misused Direct Payments, customers are moved to a commissioned service.	High	The Counter Fraud Team (CFT) will deliver a rolling programme of fraud awareness training with staff in safeguarding, financial assessments and with relevant legal services team members. Internal Audit (IA) undertake periodic review of controls which helps to ensure robust processes are in place. Suspicions of fraud are routinely investigated by the counter fraud team.
Council Tax & Business Rates Frauds (discounts and exemptions)	Council Tax fraud is a common occurrence. CIPFA reported that 65% of all local government related fraud, recorded as part of their last annual fraud survey, involved Council Tax payments. Council Tax fraud accounted for £35.9m of loss due to fraud in	The Council employs a number of methods to help ensure that only valid applications for discounts, exemptions or reliefs are accepted. This includes requiring relevant information on application forms, visits to properties (where necessary) and an annual canvass requiring businesses to confirm that	High	Council Tax and Business Rates systems are audited regularly. A new audit in the area is due to start in September 2022.

Risk Area	Risk Description	Risk Controls	Risk Category	Risk Mitigation
	2019/20 according to the survey. There are several ways in which Council Tax fraud can occur. These include applicants providing false information and recipients failing to notify the Council when they no longer qualify. Business Rates fraud does not occur as regularly but losses in this area can be much higher. The most common type of fraud that occurs is when businesses falsely claim Small Business Rate Relief discounts.	they continue to be entitled to a discount or exemption. Messages reminding residents and businesses to update their circumstances when required appear on annual bills issued by the Council. An audit of Council Tax and Business Rates received substantial assurance in 2021.		
Council Tax Reduction Fraud	Council Tax Reduction (CTR) is a council funded reduction in liability introduced in 2013 to replace Council Tax Benefit. Unlike its predecessor, it is resourced entirely through Council funds. Fraud in this area occurs regularly but is usually of lower value. Frauds can involve applicants failing to declare their total assets, correct household composition or household income. Those receiving support are also required to notify relevant authorities when they	The Council undertakes eligibility checks on those who apply for support. There are established lines of communication with the Department for Work and Pensions (DWP) where claims for support are linked to externally funded benefits. The Council is able to report Housing Benefit and other benefit frauds to the DWP but this does not necessarily allow the Council control over resolving false claims for CTR.	High	CFT to promote the review of National Fraud Initiative matches in this area.

Risk Area	Risk Description	Risk Controls	Risk Category	Risk Mitigation
	have a change in circumstances that may affect their entitlement to support.	An audit into benefits administered by the Council received reasonable assurance in 2021.		
Creditor Fraud	A range of frauds can be committed against the Council as a result of publicly available creditor payment data. Criminals undertaking these types of fraud are often found to be operating from overseas. The most common issue is mandate fraud where fraudsters impersonate legitimate suppliers and attempt to divert payments by requesting changes in bank details. Other types of fraud in this area include whaling, where senior members of the Council are targeted and impersonated in order to obtain fraudulent payments. In recent years there have been increased instances nationally of hackers gaining direct access to email accounts of suppliers and then attempting to perpetrate mandate frauds. These attempts are much more difficult to detect and prevent.	The Council has a number of controls in place to identify fraudulent attempts to divert payments from genuine suppliers and to validate any requests to change supplier details. A Creditors audit in 2020/21 found robust processes were in place, in line with the Council's Financial Regulations, and gave the area substantial assurance. CFT delivered bespoke training to staff in charge of creditors in 2022.	High	The CFT undertake work to raise staff awareness of these types of frauds. Increased awareness provides greater chances of stopping fraudulent attempts before losses occur. Regional and national fraud alerts are regularly shared with staff working in this area to help prevent this type of fraud from occurring. All instances of attempted or successful fraud reported to the CFT will be reported to the relevant agencies, such as the National Anti Fraud Network. An audit will be conducted in this area in 2022/23.

Risk Area	Risk Description	Risk Controls	Risk Category	Risk Mitigation
Cybercrime	Cybercrime is a constantly evolving area. Criminals are continually refining their techniques in order to overcome controls put in place to protect organisations. They seek to obtain unauthorised access and information, and to frustrate systems to steal or extort money or assets. Types of cybercrime experienced by local authorities in recent years include ransomware, phishing, whaling, hacking, and denial of service attacks. Attacks can lead to loss of funds, systems becoming unavailable to use impacting service delivery, and loss of data. There have been a number of high profile cyber-attacks on public and private sector organisations in recent years. Attacks stemming from the hacking of software or IT service providers have become more prevalent. These are known as supply chain attacks and are used by hackers to target the end users of the software created by the organisations targeted.	The Council has a skilled ICT department which helps mitigate the threat of cybercrime. The Council's information security procedures require the central reporting of all cybersecurity incidents; including near misses. An audit conducted in 2020/21 of cybersecurity awareness amongst staff and Members found the Council has good measures in place. A substantial assurance opinion was given.	High	Raising awareness with staff can be crucial in helping to prevent successful cyberattacks. Any counter fraud training delivered will reinforce cybersecurity messages to members of staff. Veritau undertake an annual awareness campaign highlighting cyber security issues. IA periodically conduct ICT audits that review elements of cybersecurity.

Risk Area	Risk Description	Risk Controls	Risk Category	Risk Mitigation
Procurement Fraud	Procurement fraud has been perceived as a high risk by local authorities for some time. Incidents of fraud in this area are rare but when they do occur they often carry a high level of financial and reputational damage. Procurement fraud, by its nature, is difficult to detect but can result in large scale loss of public funds over long periods of time. The Competition and Markets Authority (CMA) estimates that having a cartel within a supply chain can raise prices by 30% or more. In 2020 CIPFA found that 8% of fraud detected in this area involved 'insider fraud'.	The Council has established Contract Procedure Rules. The rules are reviewed regularly. Controls include the requirement for competitive procurement processes. A team of procurement professionals provide guidance and advice. The Middlesbrough Manager Framework includes contract management expectations for managers. The Contract Procedure Rules also set out the requirements for declarations of interest to be made.	High	Continued vigilance by relevant staff is key to identifying and tackling procurement fraud. The CFT will continue to provide training to raise awareness of fraud risks in this area. The CFT and IA monitor guidance on fraud detection issued by the Competition and Markets Authority and other relevant bodies. Audit work in this area is being considered during 2022/23.
Fraudulent Insurance Claims	The Council may receive exaggerated or fabricated insurance claims. Zurich report a rise in false claims due to the "cost of living crisis". Fraudulent claims pose a serious risk of loss to the authority.	While insurance fraud is common, the burden of risk is currently shouldered by the Council's insurers who have established fraud investigation systems. However, there are implications for the Council where insurers pass on costs relating to fraud through increased premiums.	Medium (upgraded from Low)	The CFT will explore working with the Insurance Team to assist in minimising false claims.

Risk Area	Risk Description	Risk Controls	Risk Category	Risk Mitigation
Internal Fraud	There are a range of potential employee frauds including falsifying timesheets and expense claims, abusing flexitime or annual leave systems, undertaking alternative work while sick, or working for a third party on Council time. Some staff have access to equipment and material that may be misused for private purposes. Payroll related fraud can involve the setting up of 'ghost' employees in order to divert salary payments to others. Corruption and bribery is a significant risk to all public sector organisations, however, only low levels have ever been detected.	The Council has a whistleblowing policy through which concerns can be raised. The Council has an anti-bribery policy that asks staff and members to report concerns through the whistleblowing policy. Controls are in place surrounding flexitime, annual leave and sickness absence. Participation in the National Fraud Initiative helps the Council identify potential cases of internal fraud.	Medium	The CFT will investigate any suspicions of corruption while internal audit ensure that appropriate checks and balances are in place to help prevent it.
Recruitment Fraud	Recruitment fraud can affect all organisations. Applicants can provide false or misleading information in order to gain employment such as bogus employment history and qualifications or providing false identification documents to demonstrate the right to work in the UK.	The Council has controls in place to mitigate the risk of fraud in this area. DBS checks are undertaken where necessary. Additional checks are made on applications for roles involving children and vulnerable adults.	Medium	Where there is a suspicion that someone has provided false information to gain employment, the CFT will be consulted on possible criminal action in tandem with any disciplinary action that may be taken.

Risk Area	Risk Description	Risk Controls	Risk Category	Risk Mitigation
Theft of Assets	The theft of assets can cause financial loss and reputational damage. It can also negatively impact on employee morale and disrupt the delivery of services. The Council owns large numbers of physical items, such as IT equipment, vehicles and tools.	Specific registers of physical assets (eg capital items, property and ICT equipment) are maintained. The Council's whistleblowing arrangements provide an outlet for reporting concerns of theft.	Medium	Members of staff should also be vigilant and report all possible thefts promptly to the Police and CFT.
Blue Badge Fraud	Blue Badge fraud carries a low financial risk to the authority but can affect the quality of life for disabled residents and visitors. There is a risk of reputational damage to the Council if abuse of this scheme is not addressed. People using a Blue Badge that does not belong to them and without the badge holder present are acting contrary to the law. They may also incorrectly be exempted from parking charges or pay reduced fees, in addition to being able to park in restricted areas including on many double yellow lines.	Measures are already in place to control the legitimate issue of blue badges. The Council participates in the National Fraud Initiative which flags badges issued to deceased users, and badge holders who have obtained a blue badge from more than one authority, enabling their recovery to prevent misuse. Enforcement officers make checks of badges seen in use. Where an issue is identified, the badge is confiscated and returned to the issuing authority.	Low	Periodic proactive days of action between the CFT and the Council's enforcement team are being planned. This will raise awareness and act as a deterrent to badge misuse. Instances of misuse should be reported to the CFT who can investigate any criminal misuse.
COVID-19 related fraud	During the Covid-19 pandemic local authorities were responsible	Over the course of 2020/21 the Council developed robust processes	Low (downgraded	Where payments were found to have been fraudulently or

Risk Area	Risk Description	Risk Controls	Risk Category	Risk Mitigation
	for providing support to businesses and residents. These schemes have now ended, however, the Council is still required to participate in post-payment verification activity with central government departments. Investigation of Covid-19 fraud by national bodies may identify further fraud perpetrated against the Council that is as yet undetected.	to identify fraudulent applications for support. This included use of national data matching resources. The CFT shared details of all known frauds occurring regionally and nationally. Government mandated post-assurance activities have been undertaken to review the success of controls in place.	from Medium)	incorrectly made a recovery process was instigated. Veritau conducted pre-application checks on payments made on Omicron and Additional Restriction Grant schemes.