



devon**audit**partnership

Counter Fraud Services

Counter Fraud Services

Half Year Report 2020 -
2021

Plymouth City Council
Audit & Governance
Committee

Date November 2020

CUSTOMER
SERVICE
EXCELLENCE



Support, Assurance & Innovation

1. Introduction

- 1.1 Counter Fraud work has continued throughout the current year and the Counter Fraud Team along with the rest of the wider Devon Audit Partnership (DAP) Team have supported Plymouth City Council in enabling and supporting Council business at these unprecedented times to ensure that services are provided to those with genuine entitlement.
- 1.2 It has been reported that there has been a general upturn in fraudulent activity during the COVID 19 (C19) crisis. Many frauds which are often referred to as Scams have adopted a C19 camouflage in order to play on people fears and lack of knowledge. Fraud activity had already significantly increased in the years prior to C19, therefore an accurate picture of the direct effects of the current crisis on fraud statistics will remain unclear for some time.
- 1.3 Fraud is by definition a crime and should not be tolerated. Any fraud against Plymouth City Council is a fraud against the public purse and therefore we will continue to acknowledge the threat from fraud, build processes and policies that will prevent fraud and pursue those who would commit fraud to ensure that the public retain confidence in the Council. Collaboration across the public sector will continue and strengthen under the current working arrangements through DAP and its partners.
- 1.4 The following report is a half year summary of the counter fraud work undertaken in support of Plymouth City Council.

2. Fraud Prevention and Detection

- 2.1 Counter-fraud arrangements are a high priority for the Council and assist in the protection of public funds and accountability. The Cabinet Office runs a national data matching exercise, The National Fraud Initiative (NFI), every two years. The data submission for the latest 2020/21 exercise is underway and DAP are co-ordinating the extracts of relevant Council datasets, as defined by the Cabinet Office. Departments have or are in the process of supplying their datasets (listed below) and these are being or will be uploaded onto the NFI secure website by December in accordance with the NFI timetable. The subsequent matching reports will be returned and actioned through the relevant Departments at the start of 2021.
- 2.2 PCC, datasets being matched against the NFI
- Council Tax,
 - Creditor Payments,
 - Housing Benefits, ,
 - Payroll / Pensions.
 - Housing Waiting Lists,
 - Licencing (including taxi licences and personal alcohol licences)
 - Market Traders, and
 - Transport Passes (including blue badges and concessionary bus passes)
 - Covid 19 Grants
- 2.3 Statistical analysis from the latest [NFI Report](#) released in July 2020 shows that significant savings continue to be achieved and that the average fraud value per case has risen from £2,727.64 to £2,944.23 an average increase of 7.94%.
- 2.4 The overall savings linked to the NFI exercise are recognised as significant and an important step in organisations minimising the losses to their business and the public purse.

“I am therefore delighted to report that the National Fraud Initiative, the Cabinet Office’s data matching service, has enabled participating organisations to prevent and detect £245 million fraud and error in the period 1st April 2018 to 4th April 2020. This brings cumulative outcomes for NFI participants to £1.93 billion.”

(Lord Agnew, Minister of State at the Cabinet Office and Her Majesty’s Treasury)

2.5 Irregularities – DAP have provided management with a range of advice and support on courses of action and or improvements to controls on relevant internal matters. Audit and Counter Fraud disciplines are now working closer than ever to provide as high a level of service as possible.

2.6 The statistics for the current year show that there are consistent savings to be made by countering fraud. There have been 235 allegations of fraud made so far this year resulting in 13 recommended prosecutions and 21 recommendations for Cautions and other forms of sanction. Along with various compliance visits a total savings figure of £377,146.22 has been realised at time of writing this half yearly report. The team continue to investigate 145 fraud allegations.

Case reviews are available on **Appendix A**

3. Areas of current fraud investigations

3.1 As part of its ongoing commitment to countering fraud in Plymouth, the Counter Fraud Services Team continues to undertake investigations in the following areas:

- Internal cases
- COVID 19 Grant Fraud
- Council Tax Support / Single Person Discount
- Blue Badge misuse
- Social Housing Fraud (involving our partner Registered Social Landlords)
- Client Financial Fraud (Special guardianship)
- Insurance fraud
- Bus pass misuse
- Parking Permit selling
- Disabled Facilities Grants

3.2 The Counter Fraud Services Team will continue to work closely with all PCC departments to ensure that fraud risks are minimised and wherever possible, those found committing offences are dealt with robustly and in line with PCC’s Anti-Fraud, Bribery and Corruption Policy and its linked Strategy and Response Plan.

4. General COVID19 related fraud

4.1 As previously mentioned fraudsters are taking advantage of the current pandemic in order to play on people’s fears and lack of knowledge and or understanding. The Counter Fraud Services Team have utilised the National Anti-Fraud Network (NAFN) to regularly update and assist Plymouth City Council to ensure that it and its customers are kept up to date with the detected and suspected fraud threats. The following are examples of fraud and attempted frauds that have been uncovered nationally -

- Victim alleged to have breached stay home regulations scam, fraudulent text messages from .GOV.UK issuing fines for leaving home.
- Free school meals scam, fraudulent messages to parents entitled to free school meals requesting bank details. Messages received via email and text.

- Fraudsters purporting to be from a research group that mimic the Centre for Disease Control and Prevention (CDC) and World Health Organisation (WHO). They claim to provide the victim with a list of active infections in their area but to access this information the victim needs to either: click on a link which redirects them to a credential-stealing page; or make a donation of support in the form of a payment into a Bitcoin account.
- Fraudsters providing articles about the virus outbreak with a link to a fake company website where victims are encouraged to click to subscribe to a daily newsletter for further updates.
- Lender Loan Fraud – there are already media reports circulating about parents concerned that they may not be able to feed their children if they are not at school and those who will be made redundant or self-employed receiving a much reduced income with potentially the same or increased living costs. This may mean people look to quick loans to see them through.

4.2 Where people feel that they are at risk, medically or financially, the same methods are used in an attempt to appeal to individuals need for security and stability -

- Fraudsters sending investment scheme and trading advice encouraging people to take advantage of the coronavirus downturn encouraging victim to divulge details and or click on fraudulent links.
- Fraudsters purporting to be from HMRC offering a tax refund and directing victims to a fake website to harvest their personal and financial details. The emails often display the HMRC logo making it look reasonably genuine and convincing. We have also had reports of people receiving similar text messages.
- Since lockdown eased, fake websites have offered cheap holidays abroad and at home with links that steal personal data and or encourage payment when no product is available.
- Holiday rental homes scam, where there is no rental home available.

4.3 As the crisis deepened, we became more settled in our new reality and many wanted to help others less fortunate as well as those who are on the front line during the pandemic, fraudsters took advantage of individual's good nature in the following ways.

- Scam emails purporting to be from the Government asking for donations to the NHS.
- Emails, texts, letters and telephone calls purporting to be from legitimate charities requesting financial support.
- Scam emails requesting details of individuals to sign up to volunteering schemes in the local area.

4.4 Plymouth City Council should also be aware of the following expected and emerging frauds both for their business their constituents and customers, we continue to work closely with the Trading Standards Team to ensure that's all threats are highlighted so that awareness remains high.

- Online Shopping and Auction Fraud – more people at home socially distancing increases the number of people online shopping through necessity but also the fact they have more time on their hands to browse the internet.
- Computer Software Service Fraud – more people working from home will increase demand on IT systems causing slower responses and making some scripts seem more believable.
- Mandate Fraud – with more people working at home, it may be easier for fraudsters to impersonate senior decision makers, with seemingly valid reasons why they cannot be contacted, and request a change in direct debit or standing order payments.
- Investment Fraud including Pension Liberation Fraud – fraudsters could take the opportunity to create bogus investments in commodities in high demand, for example

oxygen, and if people are worried that they might not have enough money to see them through this financially uncertain time, they may be more prepared to invest.

5. Specific C19 Grant Fraud

5.1 In response to the pandemic the Government announced there would be support for small businesses, and businesses in the retail, hospitality and leisure sectors. This support took the form of grant funding schemes, including the Small Business Grant Fund and the Retail, Hospitality and Leisure Grant Fund. There has also been a Discretionary Business Grants Fund developed separately by LA's.

5.2 Business Grants have proven a high value target for fraudsters. This has prompted a national wide response from HM Government and since the implementation of the schemes many organisations have come forward offering support, especially in the data matching and analysis area in an attempt to provide tools to LA's so that they in turn are able provide full 'Assurance' that the £20 billion spent nationally in support for businesses that –

- Only genuine claims are processed and or have been paid and
- Where claims have been identified as incorrect, false or spurious, that they have been highlighted for follow up action and or redress.

5.3 All Local Authorities will be affected by fraud in this area whether they have direct responsibility for the dispersal of funds, or not, as it is all funding from the 'Public Purse' and eventually this will affect all areas of public life in the UK.

5.4 With such large amounts of money available, it is unsurprising that opportunistic as well as organised fraudsters have taken advantage of the urgency and confusion caused by the C19 global pandemic, in order to line their own unscrupulous pockets. Below are some known successful and attempted frauds in this area of Council Business.

- Scam one: Someone emails the council pretending to be the liable party on a business rates account. They ask to be reminded what their account number is because they don't have access to the paperwork. They then use this account number to apply for a Covid-19 business grant.
- Scam two: Someone emails the council saying they moved to a new business premises in the area before March 2020. Often they use a tactic to add pressure, e.g claiming they tried to contact the council months ago, but their application form was lost. They don't have to actually pay the business rates because they've been suspended. They can access a Covid-19 business grant with the account information provided (up to £25k).
- Business owners, whose business liquidated prior to 11/03/20, attempt to claim and fail to notify that the business has folded prior to qualification. This may take the form of the owner maintaining that there is a new business taking over from the old one.

5.5 All involved LA's have a Single Point of Contact (SPOC) who is responsible for fraud reporting at the national level. Any frauds that cross LA borders or are considered related to organised crime must be reported in real time. The SPOC for Plymouth City Council is the Counter Fraud Services Manager at DAP.

5.6 National Fraud Initiative Response (NFI) A recent consultation document issued by the Cabinet Office (CO) made it clear that it is the Government's intention to ensure that Grant Payments made during the C19 crisis are included in this year's data submission for the NFI. This data will need to be submitted by Dec 2020.

- 5.7 The resultant matches/mismatches will have to be investigated, justified or corrected. Where fraud is identified it may be necessary for LA's to use the full weight of the law in order to be able to recover fraudulent debt. This may / will undoubtedly uncover more sophisticated frauds that cross LA borders.
- 5.8 The Counter Fraud Services Team are currently assisting Plymouth City Council in providing Assurance to the Department for Business, Energy & Industrial Strategy in the form of a monthly Assurance Report. A separate 'Assurance Strategy' is supported by the effective work that the relevant Departments are doing along with input from both Audit and Counter Fraud sections within DAP.
- 5.9 The Counter Fraud Services Manager will continue to act for PCC in C19 Grant Fraud related matters until resolution of all suspected or alleged frauds in this area. There are currently 9 separate investigations into this area of business with a Grant Value of £105k. The nationally detected figure for fraud in this area is so far £8 Million and increasing as more and more frauds are detected.

6. Statistical evidence

- 6.1 The problem of fraud is an ever growing one, which is constantly changing and evolving. Research shows that detected or reported examples of fraud do not represent the total cost of fraud, as much remains undetected and or hidden. Investing in the appropriate strategies means that organisations can continue to increase their resilience to fraud as this is recognised as one of the most effective ways to reduce the risk of fraud.
- 6.2 Various organisations have seen an upturn in the reporting of fraudulent activity. Whilst this is to be expected, the full extent of fraud activity will not be known for some time and the total of losses are unknown. At this time it is difficult to say whether there is more fraud activity due to C19 or whether reporting has increased and fraud has just taken on a C19 cover, whereas prior it hid in many different guises. Below are some headlines from counter fraud teams across the country.
- 6.3 We know from previous experience that reported fraud is the tip of the iceberg and that most goes undetected and or unreported as it is a hidden crime.

Action Fraud

- Animal lovers looking for pets in lockdown defrauded of nearly £300,000 in two months - Tuesday, 5 May, 2020
- Cyber experts shine light on online scams as British public flag over 160,000 suspect emails - Thursday, 7 May, 2020
- 260 reports of coronavirus-related TV Licensing emails so far this month - Wednesday, 27 May, 2020
- A total of £11,316,266 has been reported lost by 2,866 victims of coronavirus-related scams.
- Action Fraud have received 13,820 reports of coronavirus-related phishing emails. 12 June, 2020
- Over £16 million lost to online shopping fraud during lockdown - Friday, 19 June, 2020

Her Majesties Revenues and Customs (HMRC)

- More than 10,000 COVID related phishing scams are being investigated by Her Majesty's Revenue & Custom (HMRC)

- In May alone more than 5,000 scams were reported to HMRC by the public. A rise of 337% if compared to March figures, when lockdown began. During the month, HMRC asked internet service providers to remove 292 scam websites to help combat the issue.

GOV.UK

- Fraudsters are exploiting the spread of coronavirus (COVID-19) in order to carry out fraud and cybercrime. Police have reported an increase in coronavirus related scams.
- We are issuing an alert to help charities minimise the risk of becoming a victim of such frauds and cyber-attacks. All charities, but especially those providing services and supporting local communities during the coronavirus crisis, could be targeted by fraudsters.

7. Where can PCC customers get advice?

7.1 Detailed counter fraud advice is available online, including from these trusted sites. **Only use trusted sites and or those displaying that they are secure.** (site address starts with “https” or displays a padlock image next to the site address)

- [Scamsmart](#),
- [ActionFraud](#),
- [CIFAS](#),
- [TakeFive](#),
- [Citizens Advice](#),
- [Trading Standards](#)
- [National Cyber Security Centre](#).
- [Fraud Advisory Panel](#)

8. Conclusion

8.1 The DAP Counter Fraud Services Team can state that Plymouth City Council remains highly committed to its moral and legal duties to the public and that it effectively acts in line with its own ‘Plan, Mission, Value and Priorities’ where countering fraud is concerned.

8.2 Plymouth City Council has made provable Accumulated savings over the past 5 years in cashable and non-cashable savings of £6,196,659. 96 by countering fraud in all areas of its business.

8.3 Local authorities continue to face a significant and unprecedented fraud challenges. Official figures are dated, however the argument for protecting the public purse remains an ongoing priority. The National Fraud Authority (2013) estimated local authorities face the threat of £2.1bn fraud a year. In fact, the [Annual Fraud Indicator](#), produced by Crowe Clark Whitehill, estimates that figure may be as high as £7.8bn in 2017, out of a total of £40.4bn for the public sector as a whole. [The Government’s Economic Crime Plan](#) states that the numbers of fraud offences rose by 12% during 2018 to 3.6 million – constituting a third of all crimes in the UK.

It is therefore crucial to commend Plymouth City Council for the continued support and commitment that it shows in protecting the public purse year on year, especially during these extremely difficult times when every penny of public funding counts more than ever.

8.4 A full contact list for DAP Counter Fraud Services is available on **Appendix B**

COUNTER FRAUD SERVICES TEAM CASE STUDIES



Social Housing Fraudster Fined in Plymouth for unlawful sublet.



The Counter Fraud Services Team at Devon Audit Partnership are proud to report that in collaboration with Plymouth City Council (Legal Team) and Plymouth Community Homes staff, that another illegal sublet has ended and the perpetrator has been prosecuted, enabling another family home to be let out to those with a genuine entitlement who were waiting patiently on the housing list.

A woman living in Cornwall has pled guilty to an illegal sublet of her Plymouth Social Housing property for 5 years in court this week after admitting an offence contrary to the Prevention of Social Housing Fraud Act 2013 S2(1)

She left her Plymouth house in March 2014 to live with her partner in Cornwall who she later married and failed to inform her Social Landlord that she was moving out and that she would be allowing her grown up

OFFICIAL

children (who were not entitled to succession) to live there and pay the rent and utility bills, under her name.

In an attempt to hide the fact that she was acting illegally she continued to use her previous married name when dealing with authorities in Plymouth, but used her new married name when dealing with authorities in Cornwall.

She later allowed her daughter to pretend to be her in an attempt to obtain a mutual exchange so that she could obtain another social housing property by deception in the Plymouth area.

She was sentenced to a fine of £600, with a Victim surcharge of £60 and costs of £450 meaning she will have to repay £1,110.

Despite the evidence to the contrary the defendant maintained that she didn't know she was doing anything wrong, however the Magistrate stated "You also went to great lengths to disguise your behaviour" when passing sentence.

Social housing fraud is a blight on society at a time when social housing is at a premium. The monetary cost for this type of fraud is estimated to cost the public purse around £900 million annually, however the human cost for those in genuine need of a home is unmeasurable.

Katrina Robinson MBE, Solicitor and Chair of the Tenancy Fraud Forum stated that –

"This is a fantastic result from the Devon Audit Partnership and clearly shows that they are resilient and determined to stop tenancy fraud in its tracks. It's quite clear that the tenant was fully aware that what she was doing was wrong and that her children had no need for a social home with the support and significantly reduced rent that comes with that.

This sends out a clear message that tenancy fraud is not a victimless crime and the property will now be allocated to a family who need the security of a social home. If you are committing tenancy fraud in Devon, then you will be investigated and risk a prison sentence and a large fine."

Plymouth woman admits 56 Fraud Act Offences to get a Social Housing property.



Just two weeks after our last success the Counter Fraud Services Team at Devon Audit Partnership are proud to report that in collaboration with Plymouth City Council (Community Connections and Legal Teams) and Plymouth Community Homes staff, that a Plymouth woman has been convicted of lying in an attempt to obtain a Social Housing property ahead of those with a genuine entitlement waiting patiently on the housing list.

The Plymouth woman who repeatedly lied about owning a property while trying to get social housing has been given an 18 month community order at Plymouth magistrates.

The 49 year old was also ordered to perform 20 rehabilitation activity days, seek mental health treatment as well as pay £450 costs and £85 victim surcharge.

OFFICIAL

Plymouth magistrates heard Wright applied to Devon Home Choice for a social housing property in September 2017 and gave an address history back to 2011 with no reference to a property in Kirkstall Close - which she jointly owned with an ex-partner.

The following month she presented as homeless and filled in forms which stated that she did not own a property or had an interest in one. In January 2018 she put in another Devon Home Choice application with an updated address as she had moved in with her parents. Again, she gave an address history dating back to 2011 but did not include the property she owned.

In total she placed bids on 43 properties before being offered a property from Plymouth Community Homes. Each time she bid she had to confirm her details were correct and that she understood it was an offence to use incorrect information.

In May 2018, she completed a pre-tenancy assessment with PCH, but a credit search showed up an active mortgage and the offer of a property was suspended.

Over the following weeks, she repeatedly denied she had a property or a mortgage. She even got in touch with her local councillor to complain her application had been suspended.

In June 2018 her case was passed on to the Counter Fraud Services Team at Devon Audit Partnership (DAP) to investigate. She continued to deny owning a property or having a mortgage until she was shown her own mortgage account information and the land registry details. At that stage she confirmed that she must still own the property, but as she split from her ex-husband, had assumed her details had been taken off the property.

She was, however, also shown her bank account information which showed her making payments towards the mortgage and receiving payments from tenants living in the property.

She still claimed no knowledge of some of the bank accounts and argued with investigators that she only had one account and may have forgotten to close another. It was only when investigators pointed out that cash point withdrawals were being made she finally confessed that she owned the property, had arranged for it to be rented out, was paying the mortgage and receiving rent for the property.

In mitigation, she said her relationship with her ex-husband had badly broken down and she no longer wanted to live at the property they owned. She also had a very poor credit history so private renting was not possible as she would not pass a credit check. She also suffered from mental health issues.

Plymouth City Council Cabinet member for Housing and Cooperative Development Councillor Chris Penberthy said: "We have a waiting list of around 10,000 households looking for somewhere to call home. If you already own a property, you must declare it. There may be compelling reasons why you can no longer use that property, but to just repeatedly lie time after time, is just not on."

"This is fraud. This is lying to gain an unfair advantage over others who are in need. We ask people to be honest when they fill in forms for a reason."

DAP will continue to act for Local Authorities across Devon and support the Devon Tenancy Fraud Forum where required in order to ensure that those in genuine need are not cheated by this type of selfish criminal behaviour.

Appendix B

Devon Counter Fraud Services Contacts

Name	Position	Telephone	Email
Ken Johnson	Counter Fraud Services Manager	01752 307625	Ken.johnson@plymouth.gcsx.gov.uk

OFFICIAL

Pete Burgoyne	Fraud Investigator	01752 305977	<u>Peter.burgoyne@plymouth.gcsx.gov.uk</u>
Paul Clayton	Fraud Investigator	01752 305249	<u>Paul.clayton@plymouth.gcsx.gov.uk</u>
Dina Williams	Fraud Investigator	01752 307619	<u>Dina.williams@plymouth.gcsx.gov.uk</u>
Ashley Varley	Fraud Investigator	01752 304182	<u>Ashley.varley@plymouth.gcsx.gov.uk</u>
Sue Roach	Intelligence Officer	01752 307618	<u>Susan.roach@plymouth.gcsx.gov.uk</u>
Rob Rogers	Compliance Officer	01752 398556	<u>Robert.rogers@plymouth.gov.uk</u>
Fraud referral email address			<u>Corporatefraud@plymouth.gov.uk</u>
Tenancy Fraud referral email address			<u>socialhousingfraud@plymouth.gov.uk</u>
Fraud Telephone referrals		01752 304450	