To: **Audit, Risk and Scrutiny Board**

On: **23 November 2020**

Report by: **Chief Auditor**

Heading: **Audit Scotland Report – Covid-19 Emerging Fraud Risks**

---

1. **Summary**

1.1 Audit Scotland has begun publishing a series of reports relating to the Covid-19 pandemic. The first report was published in July 2020, entitled 'Covid-19: Emerging Fraud Risks', and is attached at Appendix 1.

1.2 The report highlights that since the start of the pandemic, the risk of fraud and error has increased throughout all of the Public Sector as organisations become stretched, and controls and governance are changing. The report details the range of fraud risks emerging from the Covid-19 crisis to date and provides some recommended actions which public bodies might take in order to help reduce these risks.

---

2. **Recommendations**

2.1 Members are invited to note the report from Audit Scotland, and Renfrewshire Council's arrangements which are in place in relation to the recommended actions that organisations can take to reducing the emerging public sector fraud risks.

---

3. **Background**

3.1 Covid-19 has raised significant challenges for the public sector as bodies seek to continue to deliver services for individuals, communities and businesses throughout the pandemic.

3.2 Controls and governance arrangements are likely to have had to change, and organisations may become stretched with the additional workload which has had to be undertaken in response to the pandemic. This has led to an increased risk of fraud and error throughout the public sector and across all areas of life. Audit Scotland's Report provides details of these emerging risks.

3.2 The Report is split into 3 sections: -

a) Emerging Public Sector Fraud Risks due to Covid-19
b) What Public Bodies can do to reduce these fraud risks
c) Wider Covid-19 fraud risks

4. **Emerging Public Sector Fraud Risks due to Covid-19**

4.1 The risks detailed in the report fall into the following areas: -

a) General Governance
b) Procurement
c) Covid-19 Funding
d) Payroll/Recruitment
e) IT/cyber crime
f) Health and Wellbeing

4.2 It should be noted that additional risks are likely to emerge as fraudsters will identify new ways to target public money and services.

5. **Recommended Actions to Reduce Fraud Risks**

5.1 The report highlights actions which public bodies can undertake to reduce these fraud risks. Those relevant to local authorities are summarised below along with the current and proposed arrangements in Renfrewshire Council:

- **Discuss and agree the organisation's risk appetite and associated approach to the newly emerging risks.**

  Renfrewshire's Corporate Fraud Team, Information Governance Team and Cyber Security Team are utilising resources to keep up to date with the emerging risks and liaising with the appropriate services to identify how these risks are being dealt with. They are also liaising with other local authorities and other public bodies to identify best practice in reducing these risks. Staff must continue to follow the relevant Council Policies and Procedures, for

example Financial Regulations, Information Security Policy and the Acceptable Use of ICT Equipment Policy. All User e-mails continue to be sent to staff frequently reminding them of their responsibilities in relation to information security and use of ICT Equipment. Any major breaches of policies by staff will be investigated by the relevant team.

- **Carry out a risk assessment to identify the most vulnerable areas under the new working conditions.**

  The Corporate Fraud Team are continually keeping up to date with any new Council processes, for example the small business grants and self-isolation payments introduced during the pandemic; and they liaise with the relevant services, to ensure the controls in place over the processes are adequate.

- **Ensure Internal Audit reviews systems of control**.

  Internal Audit have continued to undertake reviews during the pandemic. The 2020/2021 Internal Audit Plan has been reviewed with the assistance of Service Directors, to ensure the areas of greatest risk as a result of the pandemic have been considered. Proposed amendments to the Annual Internal Audit Plan have been submitted to the Audit, Risk and Scrutiny Board for approval.

- **Introduce new systems of control to address new and emerging risks.**

  This is completed by Services when required. Internal Audit and Corporate Fraud are regularly asked for advice when control systems are being introduced or amended and continue to liaise with services when they become aware of any emerging risks.

- **Ensure existing ways of reporting fraud or irregularity are still operating.**

  There has been no change to the methods for reporting fraud or irregularity. There is a form on the Council's website which anyone can use to report a suspected fraud and the Council has a Whistleblowing Policy in force.

- **Continue Staff training, especially for staff moved to work in areas that are new to them.**

  Staff training is actively encouraged within Renfrewshire Council and service management are responsible for ensuring their staff are adequately trained. Training was provided to those staff seconded to the local assistance teams in order to carry out the required role. During this month the Council ran its first virtual learning at work week to encourage further personal development.

- **Ensure Staff and customers receive regular, appropriate communications on the new ways of working and changes to services.**

A weekly staff newsletter is circulated to Council staff which details this information. Regular updates are also provided to staff by the Chief Executive and Service Directors and there are COVID-19 – Updates for staff on the Council's website. ICT regularly provide information to staff on new available programs and guidance on how to make best use of ICT systems in a home working environment. Renfrewshire Council's website is the main tool used to update customers on changes to Council services

- **Review the UK Government's Counter Fraud Functions website for latest guidance**

  Counter Fraud Management regular review this website for relevant reports as well as other fraud related reports from other organisations as they are well aware that they are working in an environment where the fraud landscape will constantly change. This ensures they are keeping up to date with new fraud risks and best practice for dealing with them. This information is passed on where the relevant, to other Council services. The relevant services are also liaised with, to discuss any required changes in processes which may be required to reduce certain fraud risks that emerge.

- **Consider bank account verification and active company search services**

  The Council is a member of the National Anti-Fraud Network service and uses this service to undertake bank account verification and company searches where required. This was used when the Counter Fraud Team were undertaking checks on suspected fraudulent business grant applications for grants available during the pandemic. These tools assisted in investigations which led to some suspected fraudulent grant applications being reported to Police Scotland.

- **Review the National Fraud Initiative submission requirements that will require data to be submitted related to Covid-19 payments and services**

  This has been completed and the Council will submit the required data in line with the NFI Timetable and investigate matches when the data is returned.

- **Run 'dummy phishing' exercises to test employees' reactions**

  The Council is introducing Simulated Phishing training exercises to help staff become confident in recognising malicious emails. To do this, fake phishing emails which closely mimic the real thing will be created and sent to staff. Those who do click on the link. will land on a safe page, designed by Council staff, that highlights the key parts of the email that indicate it is malicious.

- **Rotate employees or volunteers working with vulnerable service users and ensure appropriate employee disclosures are up to date.**

  The Council has a disclosure policy in operation which must be followed. A recent Internal Audit review highlighted that both staff and volunteers are subject to disclosure checks as necessary.

6 **Wider Covid-19 Fraud Risks**

6.1 Covid-19 could result in an increase in fraud across all areas in life.

6.2 The main areas of concern for members of the public is that they may receive fraudulent texts, e-mails, telephone calls or a visit from someone, posing to be someone else in an attempt to gain personal and financial details to be used in fraudulent schemes.

6.3 The Council's Trading Standards Service regularly publish helpful advice for the public on scams and provide details of what action to take if a person is subject to a scam.

Implications of the Report

1. **Financial** - The Council has in place arrangements to attempt to recover any fraudulent financial overpayments

2. **HR & Organisational Development** - None

3. **Community Planning –**
Wealthier and fairer – The Council has policies and processes in place to prevent and detect fraud and error in order to direct council resources to the correct people.

4. **Legal** - None

5. **Property/Assets** - None

6. **Information Technology** - None

7. **Equality & Human Rights** - None

8. **Health & Safety** – None

9. **Procurement** - None

10. **Risk** – Protecting Internal Resources from Crime and Information Handling are Corporate Risks of the Council

11. **Privacy Impact** – None

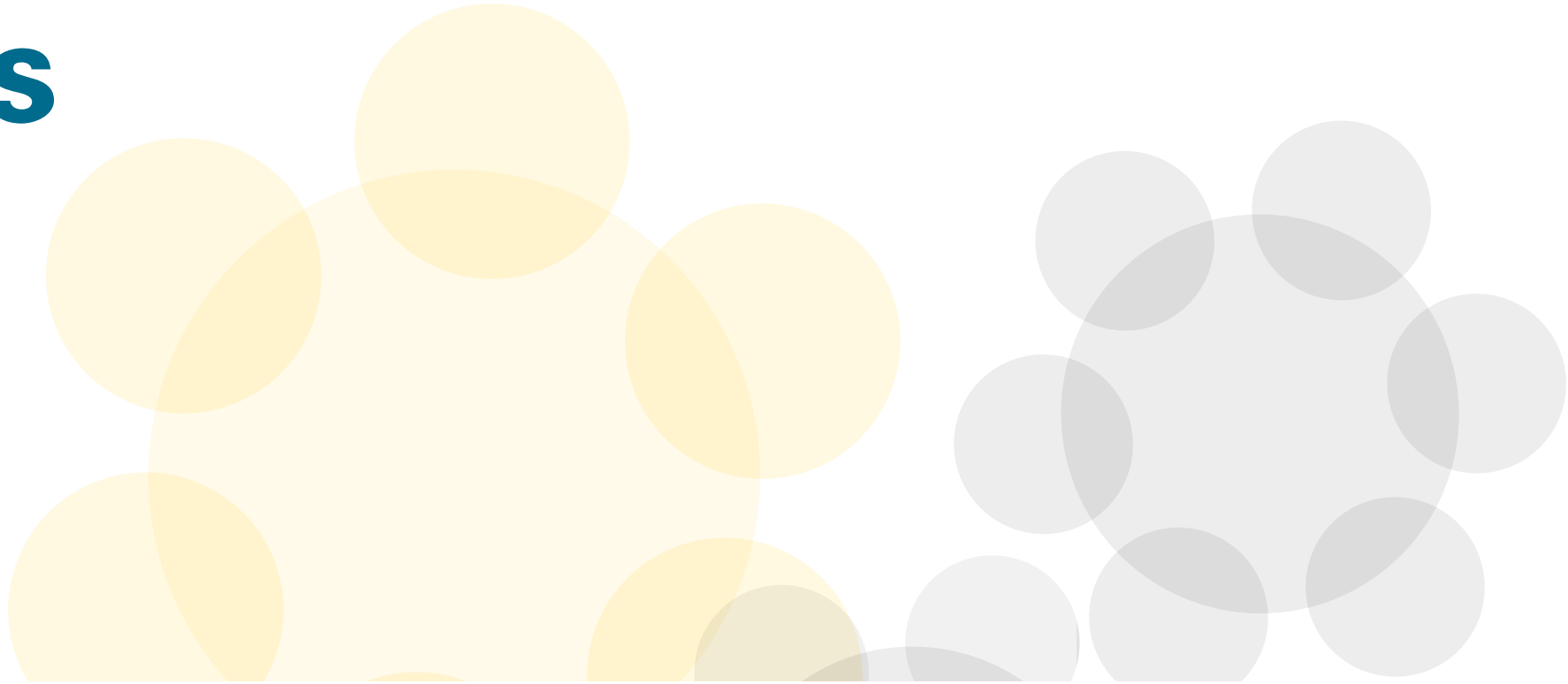
12. **COSLA Implications** – None

13. **Climate Risk** - None

Author: Andrea McMahon – 07983852046

Covid-19

Emerging fraud risks



AUDIT SCOTLAND

Prepared by Audit Scotland for public bodies and auditors
July 2020

Covid-19: Emerging fraud risks

The Covid-19 pandemic has brought significant challenges across the Scottish public sector as bodies seek to deliver services for individuals, communities and businesses in an extremely difficult time.

Since the start of the pandemic, the risk of fraud and error has increased as organisations become stretched, and controls and governance are changing. These risks are emerging for a range of reasons including:

- public-sector staff working remotely and under extreme pressure
- an increase in phishing emails and scams which try to get staff to click on links which allow fraudsters to access public-sector systems
- government stimulus packages to support individuals and businesses being provided quickly, possibly with a lower level of scrutiny and due diligence than has previously been in place for similar schemes.

This briefing sets out a range of fraud risks emerging from the Covid-19 crisis, and what public bodies might do to help reduce these risks. It aims to raise awareness of these new fraud risks with public bodies and their auditors; and support them in identifying and managing these risks, and ensure that sound governance and controls are in place.

Additional risks will continue to emerge as fraudsters identify new ways to target public money and services. Public bodies and auditors should stay alert to new scams and approaches by fraudsters, and regularly review their controls and governance arrangements to ensure they remain fit for purpose.

The information in this briefing is based on our professional judgement in auditing risk factors in the public sector. We would like to thank colleagues in Police Scotland, NHS Scotland Counter Fraud Services, local government chief internal auditors and fraud investigators for their support in preparing this briefing.

1. Emerging public sector fraud risks due to Covid-19

Covid-19 has raised significant challenges for the public sector. In such emergency situations, existing controls may be compromised, and it can be difficult to put in place robust controls for new processes. Good governance and sound controls are essential in such crisis situations. The risks include, but are not limited to:

General governance risk | Procurement risk | Covid-19 funding | Payroll/recruitment risk | IT/cyber crime risk | Health and wellbeing risk

Public sector staff are working under extreme pressure which may mean some internal controls are suspended or relaxed

Staff may be transferred from their own departments to other areas experiencing resource pressures. This may leave some departments under-staffed at the same time that inexperienced staff may be working remotely without a full understanding of the required procedures and controls

There is a risk of weakened governance arrangements as internal audit teams are redeployed to operational areas

Mandate and diversion fraud[1] may increase as fraudsters try to get employees to update bank details and make payments to suppliers as soon as possible, knowing that staff are under pressure and that the normal controls may have been relaxed

Procurement fraud could increase as normal controls may be relaxed to allow bodies to buy goods or services which are required urgently, possibly from new suppliers

An increase in medical and sanitary waste may see criminals attempt to gain waste management contracts. This could result in the inadequate disposal of the waste, with the potential associated harm to public health as well as generating proceeds for the criminals

Duplicate payments are possibly not detected, or payments may be made without checking goods and services were received to a satisfactory quality

Fraudsters may be 'selling' popular and/or hard to get items online. The products may not arrive or may turn out to be counterfeit, eg medicines, PPE and hand sanitiser products that are unsafe and do not provide the necessary level of protection

Note 1. Mandate fraud is when an employee is deceived into changing bank payment details (eg, of a supplier) in order to divert payments to fraudsters.

General governance risk | Procurement risk | Covid-19 funding | Payroll/recruitment risk | IT/cyber crime risk | Health and wellbeing risk

Government stimulus packages to support individuals and businesses are being provided quickly, possibly with a lower level of scrutiny and due diligence than has previously been in place

Councils may receive Freedom of Information requests asking for details that may be used for business grant applications. Fraudsters are possibly looking to identify eligible businesses that have not applied for grants, with a view to putting in a fraudulent application

Councils may receive fraudulent email enquires purporting to come from national companies asking for property details, reference numbers, etc, possibly with a view to making fraudulent applications for Covid-19 business grants

There is a risk that applications for Covid-19 related support due to being made online, are made using fraudulent documents and details

Councils may receive requests for business rate liabilities to be changed. This may be an attempt to ensure a business falls within a category qualifying for grants

There is a risk of recruitment fraud as new staff are needed immediately due to increased demands for services and the normal checks may not be completed

Payroll fraud may increase as normal controls around expenses, overtime, etc may be relaxed

Staff returning to work in the NHS to help respond to Covid-19 may be targeted by unscrupulous tax avoidance schemes

General governance risk | Procurement risk | Covid-19 funding | Payroll/recruitment risk | IT/cyber crime risk | Health and wellbeing risk

Staff working remotely may pose potential security risks, eg when using personal devices and/or using removable devices to download data. Household members may gain unauthorised access to confidential information such as payroll, social work client details, etc, via screens or in documents used by staff

There is a risk of increased cyber crime as more public-sector staff connect remotely to access systems and for meetings using online video conference services

Staff working remotely may receive calls from fraudsters claiming to be legitimate technical support services and attempting to gain access to systems

There is a risk of an increase in phishing[1] emails and scams trying to get staff working under pressure to click on links which allow fraudsters access to public-sector systems

There is a risk of more system access breaches where personal information is accessed without a valid reason by staff working remotely, eg possibly to check friends' applications for services

More remote working may result in isolation and /or mental health issues which could lead to increased addictive behaviours (eg, gambling), which could result in vulnerability to serious organised crime gangs

An increase in internal fraud in public bodies is possible as employees and their families are under increased levels of financial and health pressures

Working for sustained periods of time at high levels of demand may lead to errors or fraud due to lapses in concentration

Employees/volunteers could take advantage of vulnerable service users, eg by gaining access to bank cards, cash drop-offs at client's house, befriending with sinister intentions

Note 1. Phishing is where criminals send emails purporting to be from reputable sources in order to deceive individuals into providing information or data such as passwords, user names or bank details.

2. What public bodies can do to reduce these fraud risks

- Discuss and agree the organisation's risk appetite and associated approach to the newly emerging risks
- Carry out a risk assessment to identify the most vulnerable areas under the new working conditions. This will include a review of IT system security for remote working
- Ensure Internal Audit reviews systems of control. Some of the existing controls are unlikely to be still relevant and appropriate
- Introduce new systems of control to address new and emerging risks
- Ensure existing ways of reporting fraud or irregularity are still operating and are promoted, eg fraud hotlines and whistleblowing processes are still operating
- Continue staff training, especially for staff moved to work in areas that are new to them
- Ensure staff and customers receive regular, appropriate communications on the new ways of working and changes to services
- Review the NHS Counter Fraud Authority's guidance including: Covid-19 counter fraud guidance
- Review the UK Government Counter Fraud Function's website for latest guidance including Covid-19 Counter fraud response team and Fraud Control in Emergency Management:Covid-19 UK Government Guidance
- Consider bank account verification and active company search services, eg that are available from the Cabinet Office or NAFN[1] to the UK public sector
- Review NFI[2] submission requirements that will require data to be submitted related to Covid-19 payments and services
- Run 'dummy phishing' exercises to test employees' reactions, with a requirement to revisit training modules if an employee 'fails'
- Rotate employees or volunteers working with vulnerable service users and ensure appropriate employee disclosures are up to date

Notes:

1. NAFN is a shared service organisation open to all public-sector organisations. NAFN provides data, intelligence and best practice services for member organisations.
2. NFI is the National Fraud Initiative, an exercise that matches electronic data within and between public and private-sector bodies to prevent and detect fraud.

3. Wider Covid-19 fraud risks

Covid-19 could unfortunately see an increase in fraud across all areas of life.

Texts may be received advising recipients that they are eligible for a tax refund under the Self-Employment Income Support Scheme. Recipients are asked to click on a link which leads to a fake HMRC website where they are asked for personal and financial details

Texts may be received posing as coming from the NHS contact tracing service. The texts advise people they have been in contact with someone with symptoms of Covid-19. The texts direct the recipient to a website which attempts to obtain personal details

Blackmailing and phishing emails may be received, telling victims that family or friends will be infected with Covid-19 if they do not pay

Fraudulent emails may be received telling people they can claim a tax refund to help with Covid-19 financial challenges. Recipients are asked to submit personal and financial details

Cold callers posing as the NHS contact tracing service may call people to advise that they have been in contact with someone who has tested positive for Covid-19. The caller may ask the recipient for bank details to pay for a Covid-19 test

Texts may be received advising that a 'Covid-19 Home Testing Team' will visit your home and that you will need to wait in a separate room while they put on protective clothing. This is an attempt by fraudsters to gain entry to people's homes

Texts posing as coming from the local council may be received, eg asking local residents to pay for food boxes which are being delivered to families with children eligible for free school meals

People may receive telephone calls from fraudsters posing as police officers to tell them that they have breached Covid-19 restrictions and have to pay a fine

Special offers may appear online containing malicious links that users click to allegedly receive free or discounted goods

With the possible increase in online gaming during lockdown, criminals may be developing more sophisticated ways of attacking online gaming systems

Fraudsters may be posing as council, NHS or charity staff and taking money from people to buy shopping which is never delivered

Fake and malicious apps purporting as providing Covid-19 information and trackers may start emerging

There is a risk of online child sexual exploitation increasing as children spend the majority of their time online during the lockdown, either during their spare time or while receiving education

Criminals may exploit loneliness during lockdown by looking through online dating profiles in order to commit romance crime[1]

During lockdown, illicit or prescription drug use may have increased which in turn pushes prices up due to a lack of availability. The pandemic may induce 'panic buying' from different suppliers and stockpiling, leading to possible increased consumption or consuming substitute or contaminated drugs

Under lockdown, illegal drug producers may have been manufacturing pills in preparation for the summer and festivals. As a result they may have significant stockpiles of drugs, which could see the market being flooded with cheap drugs as soon as lockdown eases

Note 1. Romance crime is the engineering of a supposed friendship or relationship for fraudulent, financial gain. This may involve, for example, gaining access to the victim's bank accounts.

4. If you see or suspect fraud or would like to find out more...

Please visit the Audit Scotland counter-fraud hub

Report fraud or illegal activity to Police Scotland

Police Scotland – Keep Secure Online

Police Scotland – Reporting Cybercrime

Trading Standards

NHS Scotland Counter Fraud services

Information

You can find our reports and other material on counter-fraud on our **website**

Contacts

Anne Cairns
acairns@audit-scotland.gov.uk

Angela Canning
acanning@audit-scotland.gov.uk

Covid-19: Emerging fraud risks

This report is available in PDF and RTF formats, along with a podcast summary at:
www.audit-scotland.gov.uk

If you require this publication in an alternative format and/or language, please contact us to discuss your needs: 0131 625 1500 or **info@audit-scotland.gov.uk**

For the latest news, reports and updates, follow us on:

AUDIT SCOTLAND

Audit Scotland, 4th Floor, 102 West Port, Edinburgh EH3 9DN
T: 0131 625 1500 E: **info@audit-scotland.gov.uk**
www.audit-scotland.gov.uk