ITEM No …14……..

REPORT TO: SCRUTINY COMMITTEE – 23 SEPTEMBER 2020

REPORT ON: COVID-19 EMERGING FRAUD RISKS

REPORT BY: EXECUTIVE DIRECTOR OF CORPORATE SERVICES

REPORT NO: 214-2020

1 PURPOSE OF REPORT

To provide elected members with a summary of the above national briefing that has been compiled by Audit Scotland for public bodies and auditors.

2 RECOMMENDATIONS

It is recommended that the Committee: -

- note the key messages arising from the Audit Scotland briefing.

3 FINANCIAL IMPLICATIONS

There are no direct financial implications arising from this report.

4 MAIN TEXT

4. 1 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.

4.2 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.

4.3 The report is split into four sections. Section 1 sets out a list of specific emerging risks. These are categorised into:-

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

4.4 The report on Covid-19 Recovery Risk Register approved by Policy and Resources Committee on 24 August 2020 (Report No. 193-2020) identifies twenty key risks which address all these themes either directly or indirectly.

4.5 Section 2 considers what public bodies can do to reduce these fraud risks. A number of specific suggestions are made primarily arising from the need to maintain sound risk management and internal controls.

4.6 Section 3 covers the wider fraud risks to the general public. The Council has been highlighting these and other examples through regular updates on Covid-19 Frauds and Scams.

4.7 Section 4 provides a list of national contacts to who suspected frauds can be reported.

5 POLICY IMPLICATIONS

This report has been subject to an assessment of any impacts on Equality and Diversity, Fairness and Poverty, Environment and Corporate Risk. There are no major issues.

6 CONSULTATION

The Council Management Team were consulted in the preparation of this report.

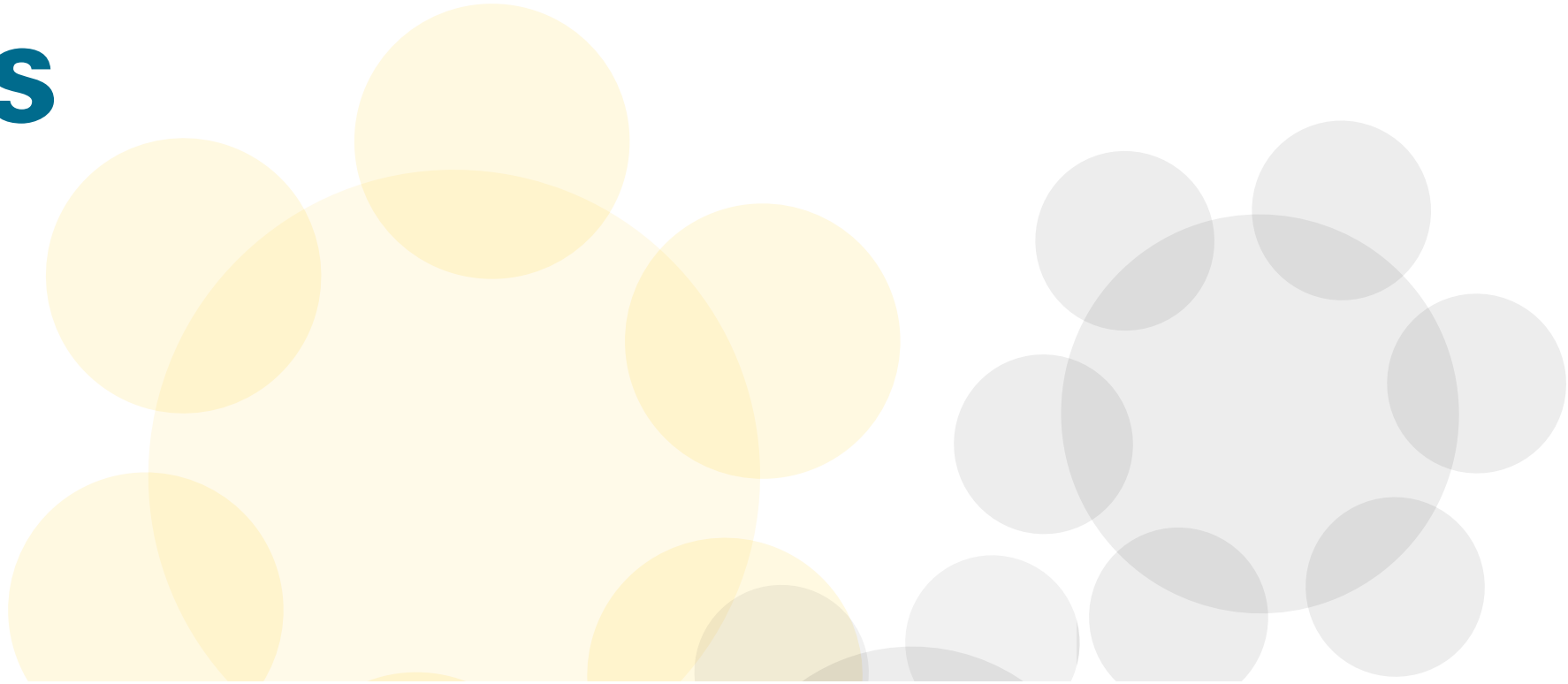
7 BACKGROUND PAPERS

None

GREGORY COLGAN
EXECUTIVE DIRECTOR OF CORPORATE SERVICES **01 SEPTEMBER 2020**

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