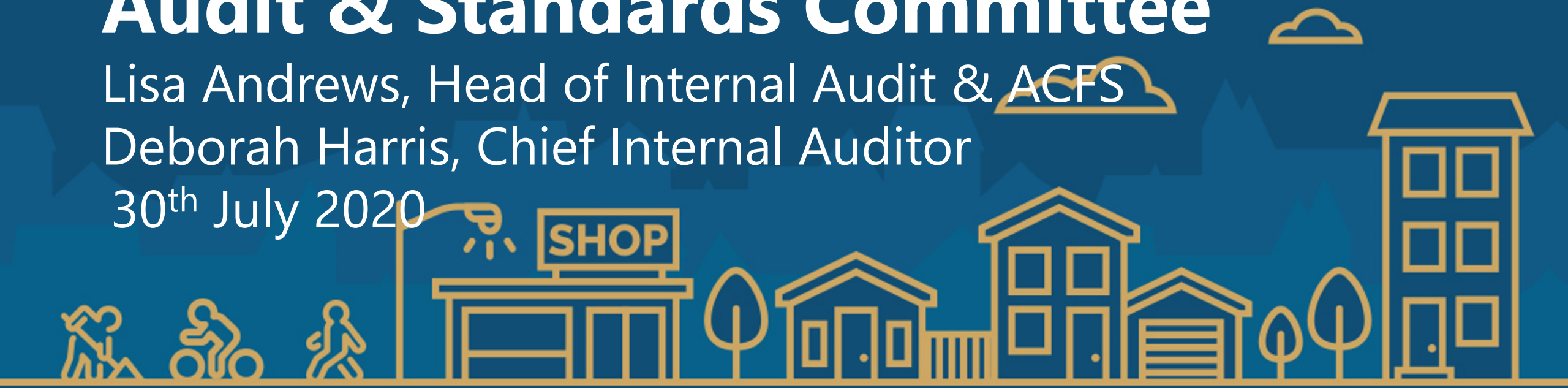
Staffordshire County Council

Fraud Risks: The Impact of COVID 19

Audit & Standards Committee

Lisa Andrews, Head of Internal Audit & ACFS
Deborah Harris, Chief Internal Auditor

30th July 2020



Introduction – Impact of COVID 19

- Criminals love **uncertainty**, **vulnerability** and **disruption** - The COVID-19 crisis provides an abundance of all three!
- COVID-19 is a huge distraction for management and employees - Many organisations have had to adapt quickly to **changes in working practices and protocols** such as remote working and increased use of digital channels. These changes present opportunities for fraudsters to exploit.
- Incentives to commit fraud may also be heightened with organisations and individuals facing unprecedented economic challenges.
- Criminals will look to seek out **weak spots** and will take advantage of 'flimsy controls' and poor IT security.
- Staying one step ahead of fraudsters can help minimise the potential damage.

Emerging Fraud Risks

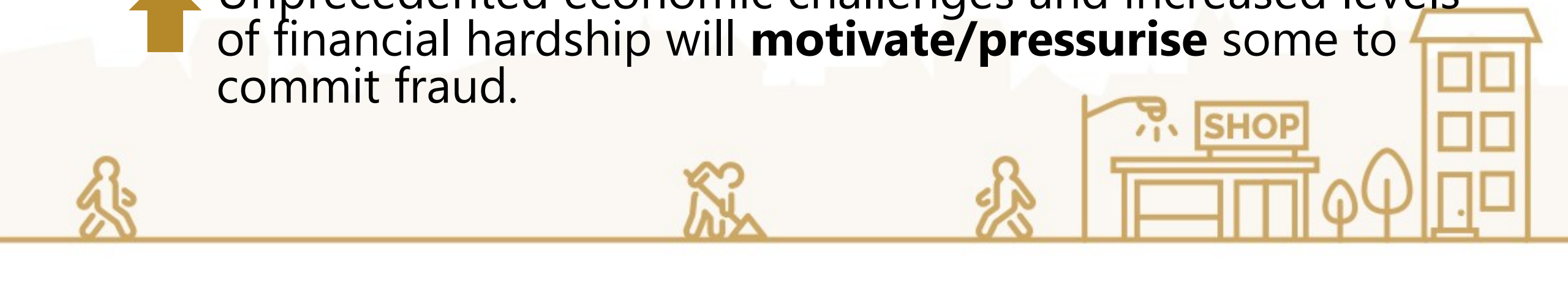
During the COVID 19 crisis, the risk of fraud increases because of the following factors:

- **Urgency in Delivery**
  Implications for due diligence and verification checks
- **Working with New Suppliers/partners or existing suppliers in new ways**
  Due diligence and verification at pace
- **Staff redeployed to COVID-19 response/increased sickness & absence level**
  - impact on segregation of duties and monitoring;
  - impact on Internal Audit and Counter Fraud Teams;
  - impact on BAU activities; and
  - staff taking on unknown roles.
- **Increased levels of remote working**
  - impact on information security;
  - impact on oversight/monitoring.
- **Increased levels of financial hardship/uncertainty**
  - impact on motivation and rationalisation to commit fraud

The Perfect Storm

The Fraud Triangle – COVID 19

- Disturbances in normal business processes, controls and working conditions give criminals **increased opportunities** to commit fraud.
- Chaos and uncertainty of the crisis enable many to **rationalize** bad behaviour that might otherwise have been checked by ethical codes.
- Unprecedented economic challenges and increased levels of financial hardship will **motivate/pressurise** some to commit fraud.



Fraud Scenarios to Look Out For

- Here are some of the fraud scenarios we are seeing right now, which are likely to flourish over the coming months and possibly well beyond the pandemic:

Bank Mandate Fraud	Bank Mandate fraud occurs when someone requests the Council to change the bank mandate, by purporting to represent an organisation we make regular payments to, for example a supplier. Fraudsters will look to identify suppliers of services the Council use on a regular basis. This can be obtained from details of contracts awarded or other information which is published on websites in line with the local transparency code. Bank mandate fraud is frequently used by serious organized crime groups as it carries low risk and potentially high rewards. In addition, Councils such as ours are particularly at risk due to (i) the high volume of transactions; (ii) the opportunity to obtain a significant sum of money in just one transaction; (iii) the disruption in terms of changes to working practices and protocols and staffing as a result of the COVID 19 pandemic .
Impersonation Fraud	Impersonation fraud happens when a fraudster pretends to be someone else and uses false details to claim for assistance e.g. small business grants and micro grants or claiming to be staff or volunteers. The COVID 19 pandemic, has seen the opportunity for small businesses to apply for micro grants from the Council as well as the recruitment of external volunteers in the provision of care support and therefore the risk of fraud is heightened.

More Fraud Scenarios to Look Out For

Application fraud

Application fraud is usually defined as when an individual uses their own name to apply for financial support, but uses false information or counterfeit documents in the application. Application fraud may involve:

- individuals falsely claiming assistance ; and/or
- companies falsely claiming assistance .

Cyber-Enabled Fraud

Cyber-enabled crimes are traditional crimes, which can be increased in their scale or reach by use of computers, computer networks or other forms of information communications technology (ICT). Unlike cyber-dependent crimes, they can be committed without the use of ICT. Two of the most widely published instances of cyber-enabled crime relate to fraud and theft. As a result of the COVID 19 pandemic there has been an increase in *"Phishing"* scams which refer specifically to the use of fraudulent emails disguised as legitimate emails that ask or *'fish'* for personal or corporate information from users, for example, passwords or bank account details. Phishing attempts can be sent out en-masse to a range of potential targets, but in the case of *'spear-phishing'*, attackers may gain specific information about a target and tailor communications accordingly to increase the chances of success.

A form of phishing, is *"smishing"* and this is when someone tries to trick you into giving them your private information via a text or SMS message. Smishing is becoming an emerging and growing threat in the world of online security.

Procurement & Supply Chain Fraud

Throughout the supply chain – from procurement to distribution – employees as well as external parties (such as suppliers, distributors and competitors) have opportunities to commit procurement fraud. These opportunities range from false invoicing, bribery and kickback schemes to non supply and/or sub-standard goods.

The COVID 19 pandemic increases the risk of this type of fraud occurring and has been seen in the procurement of Personal Protective Equipment (PPE) across the globe. There is a risk of :-

- fictitious or unqualified companies entering the supply chain;
- overcharging or duplicate claims by existing suppliers; and
- exploitation of single sourcing to use related companies



The Supply Chain – Further Considerations

Government Publication of new **Public Procurement Notices**

PPN01/20: to respond to COVID-19:Responding to COVID-19 (procuring goods, works, services in extreme urgency)

PPN02/20: Supplier Relief due to COVID-19 (guidance on payment of suppliers to ensure continuity of service)

PPN03/20: use of purchasing cards during COVID 19 and links to PPN02/20 and the payment of suppliers quickly

PPN04/20: Recovery and transition from COVID 19 - Updates and builds on the provisions contained in PPN 02/20 relating to payment of suppliers and service continuity.

Challenges of balancing:

Delivery at Pace

Due Diligence & Verification

COVID 19 Related Frauds – It’s started

There's been a 400% rise in fraud related to COVID-19 in March according to [Action Fraud]

Camden man, 20, pleads guilty to coronavirus texts scam by tricking vulnerable into handing over bank details

Scammers turn to LinkedIn to sell overpriced PPE

Teenager arrested over Covid-19 fraud claims

The suspected offender was receiving six separate Covid-19 Pandemic Unemployment Payments into a bank account, in what are believed to be bogus names.

Doing the Basics Right & Well

Prevention is key to fighting fraud and corruption both now and in the future.

Don’t forget the basics and good habits that the Council already has:

- supplier due diligence and set up;
- Robust verification on requests to change bank accounts;
- conflict of interest checks; and
- communicate that fraud will not be tolerated and how to report concerns.

Just because it’s a crisis situation, doesn’t mean everything is URGENT

Ensure that all decisions are documented to:

- allow for verification post crisis;
- ensure transparency in decision-making; and
- protect yourself and the organization



Summary - Emergency Management

The UK Government is responding to the emergency which is the COVID 19 pandemic with a range of stimulus packages to mitigate the economic and social impact of the COVID-19 pandemic.

Sadly, fraudsters will try to take advantage of these emergency measures. The fraud threat posed during emergency situations is higher than at other times, and the Council should be attuned to the risks faced by our organisation.

WHY : Financial Impact of Fraud on Organisation **v** Emotional Impact of Fraud on People

Fraud Control During Emergency Management

The following principles apply to effectively controlling the levels of fraud in an emergency management situation:

- **Accept** that there is an inherently high risk of fraud, and it is very likely to happen.
- **Understand** the fraud risks – Specifically, Internal Audit has enhanced it's fraud risk register to consider the impact of COVID 19 on SCC's anti-fraud measures and to identify further mitigating actions.
- **Consider** where controls may be weakened and implement low friction counter measures to prevent fraud risk as much as possible.
- **Carry out** targeted post-event assurance to look for fraud – Use of data analytics
- **Be mindful** of the shift from emergency payments into longer term services and revisit the control framework, as appropriate

Seek support from Internal Audit, as necessary – We are here to help and support services and we can assist with all of the above. We are assisting many services right now



Final Message

Be Diligent

Stay Vigilant

Protect Public Funds