rmp

# Risk control

## Fraud

In partnership with

GALLAGHER BASSETT
GUIDE. GUARD. GO BEYOND.

**Risk Management Partners**
rmpartners.co.uk

# Fraud

## Introduction

For public sector organisations every pound lost through fraudulent activity is a pound that potentially could have been spent on essential front line service delivery. Protecting financial resources is essential and why proactive steps are required to safeguard against fraud from external sources.

Additionally, organisations must not neglect the very real risk that fraudulent acts may be perpetrated from within.

Employers place a great deal of trust and confidence in their workforces and can sometimes fail to recognise the signs that there could be a breach of that trust. The control framework for internal fraud risk management should be as robust as that in place for external fraud.

## Employee Fraud

Employee fraud can range from the misappropriation of small stationery items, to inflated expense claims, to significant payroll fraud involving a number of employees.

The latest KPMG Fraud Barometer[1] reported:

- Total value of alleged fraud cases of over £100k reaching UK Crown Courts in 2023 reached £992.9 million
- Total volume of alleged fraud cases of over £100k increased marginally from 221 cases in 2022 to 226 in 2023
- The public sector was the most common fraud victim type by value

With widespread concern over the significantly increased cost of living in the UK over recent times, with more people and families struggling to make ends meet, it is reasonable to predict that these continuing financial pressures may be an added driver of employee fraud cases in the future.

But it is not just the direct financial losses from employee fraud that need to be considered. UK finance[2] suggests that additional costs should also be considered, including:

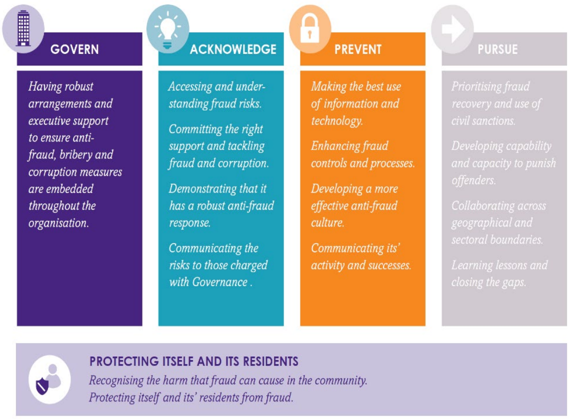
- Costs of investigating the fraud
- Costs of staff suspensions / absence
- Internal disciplinary costs
- External sanctions costs
- Permanent staff replacement costs
- Intangible costs - damage to reputation, reduced staff morale etc.

## Fighting Fraud

The Fighting Fraud and Corruption Locally (FFCL) 2020 Strategy[3] was developed by local authorities and counter fraud experts. This strategy is supported by CIPFA and is the definitive guide for council leaders, chief executives, finance directors and all those with governance responsibilities.

The most recent strategy has built on existing good practice across local government and includes recommendations for a more co-ordinated response to fighting fraud within local authorities on a local level.

The strategy sets out a governance framework of pillars of activity for local authorities to concentrate their fraud management efforts on as well as tools to support implementation and case studies of successful fraudulent convictions.



GOVERN

*Having robust arrangements and executive support to ensure anti-fraud, bribery and corruption measures are embedded throughout the organisation.*

ACKNOWLEDGE

*Accessing and understanding fraud risks.*

*Committing the right support and tackling fraud and corruption.*

*Demonstrating that it has a robust anti-fraud response.*

*Communicating the risks to those charged with Governance .*

PREVENT

*Making the best use of information and technology.*

*Enhancing fraud controls and processes.*

*Developing a more effective anti-fraud culture.*

*Communicating its' activity and successes.*

PURSUE

*Prioritising fraud recovery and use of civil sanctions.*

*Developing capability and capacity to punish offenders.*

*Collaborating across geographical and sectoral boundaries.*

*Learning lessons and closing the gaps.*

PROTECTING ITSELF AND ITS RESIDENTS

*Recognising the harm that fraud can cause in the community.*
*Protecting itself and its' residents from fraud.*

For internal fraud prevention, public sector organisations should ensure they have a robust and effective internal control framework in place and that they proactively work to identify any potential weaknesses and test their processes and procedures. Auditing, performance monitoring, and well-established risk reporting procedures will all help to strengthen internal fraud prevention standards.

## Successful Prosecutions

Local authorities regularly publish successful fraud convictions they secure which highlights their zero-tolerance approach to fraudsters stealing from the public purse. There are cases where the fraud is perpetuated by individuals within the authority.

In a standout case from 2019[4], seven housing benefit assessors were convicted after stealing more than £1m from three London authorities: Lambeth, Kingston, and Barking and Dagenham. The employed assessors created false housing benefit claims and sent the funds to accounts they controlled themselves. The fraud spanned a period of six years. The criminal activity was sophisticated, using council systems to generate council letters and set up appointments for the fraudsters at the council. Following a three-month trial, the fraudsters were sentenced to prison for a total of 17 years.

## Dynamic Operating Models

Many organisations have now adopted dynamic operating models where people may work from home permanently or on a part-time basis. These models have increased reliance on IT technology which has proven to be extremely attractive for cyber criminals who are seeking to capitalise on extended IT networks by exploiting weaknesses in organisational defences[5].

QBE Europe have set out a list of their top tips for you to effectively manage your own fraud risk:

**Fraud Protection**

**Scams**

Organised crime has made a fortune from fraud, especially in the last few years. In commercial business, cybercrime is fraud. A large amount of this fraud is driven not by advanced cybercrime but by simple scams. Users have come to rely on, and trust, technology, and the internet so scammers are increasingly looking to take advantage of what are often low-trust systems, (such as email) to deceive their victims and commit fraud.

Every fraud starts with a communication. The principal method of scamming continues to be email. Whilst most government systems employ a range of security measures to block phishing and other scam emails, some do still get through. It is an unfortunate fact that attackers hijack the mailboxes of trusted third parties and use these to send scam messages to government employees and these may not be detected leaving the recipients as vulnerable as the senders.

Working from home also introduces further vulnerability where processes and technology, which may have offered some safeguards against fraud, will no longer be effective against attackers who are able to take advantage of the situation using the methods of attack described below.

As a result, it is vital that all communications are viewed through a lens of suspicion. If a message is unexpected or contains an unusual call to action, is requesting an immediate payment, inviting a file share, or asking the recipient to follow a link, it may well be a scam. Confirm the validity of such messages with the sender and do not rush! The 'call to action' ploy is often a sign of malice, and legitimate communicators will always be happy that you took the trouble to double check.

- **Methods of Attack**

  Fraudsters have always sought to constantly evolve the methods they use to stay one step ahead of fraud prevention. Modern frauds are usually a combination of a few different, integrated scamming techniques, such as:

- **Phishing** by email or other method is rarely used in and of itself. It is part of the information gathering step and just the prelude to the attack. The aim of phishing is to obtain a victim's login credentials. Because users often set a common password for every system they access, it means that if attackers phish the credentials for one system, they are highly likely to be able to use them on many other systems. The main targets include online (cloud) services such as Microsoft 365, Google Suite, accounting systems, online shopping, as well as remote access to business systems. Frauds flow from this point because once the attackers have obtained unauthorised access to the systems used by key staff or their suppliers, they are then able to use this as a staging post to launch monitoring and scamming activity to target key staff or third parties into revealing their credentials, and finally into making fraudulent payments
- **Social Engineering** by telephone, usually in combination with email. By faking the identity of someone who the victim believes, often by invoking in them a need for urgency through a call to action or by building trust in a series of legitimate enquiries. This way, the fraudsters convince the victim to make or authorise a payment, bypass protective procedures or grant them access to their systems
- **Fake Domains** by registering domains for fake websites and email addresses which are like those of legitimate organisations, fraudsters attempt to deceive victims into diverting expected payments to fraudulent beneficiary accounts. Usually, this method includes the use of fake invoices

- **Data Encryption and Data Theft** through unauthorised use of credentials stolen via phishing attacks. A substantial proportion of all ransomware attacks occur using stolen credentials to remotely access company networks

  Data is then copied, either manually or automatically, and ransomware deployed to encrypt the victim organisation's systems. Extortion demands then encourage payment in return for often hollow promises to provide decryption keys or to prevent the release of stolen data.

  **Vital Protections**

  Like any good approach to security, the most effective protection is achieved through a multi-layered solution. Then, if one defence fails, others will still prevent loss. Ensure all the following safeguards are acting in concert:

- Whilst technical solutions to detect and block phishing messages cannot be solely relied upon, they still provide a significant protection and are vital. Ensuring proper configuration of such technologies is key to their effectiveness, and so skilled technical specialists are needed
- Staff awareness through fraud prevention training and regular phishing tests add another important control – risk-aware staff are the first line of defence. Raising risk awareness and restricting personal use of work technology can help limit exposure to some threats transmitted via social media, shopping channels, personal web-based email etc.
- Staff must use unique strong passwords for each system they access. There are a range of ways to accomplish this using both manual, memorable techniques and / or with easy-to-use password manager apps. Staff should be reminded not to share their passwords with anyone
- Strong authentication using one-time codes (often called multi-factor authentication) means that even if credentials are phished, the user accounts will remain resilient to attack
- Domain name registration. Seek to register all close domain variants. If possible, choose a domain that is quite resilient to variation by making it as short as possible
- Implement strict segregation between those who raise payments or arrange procurement and those who release payments or authorise expenditure
- Implementing rigorous data backup regimes ensuring all data is saved in multiple locations which are not accessible to ransomware. Simple tape backup being one such option
- Minimising authorised data access. Ensuring that users only have permissions to the data and applications needed for their specific job activity and that such permissions are revoked as soon as staff change role or leave the organisation. If accounts are compromised the losses are minimised
- Inadvertent sharing of data with a fraudster mimicking a colleague, authority figure, or a trusted third party, can sometimes be the basis of extortion or manipulation into committing crime so absolute care is needed when handling or transferring data. Internal links should be used instead of emails and the need to send data externally, even if encrypted, should always be questioned. Double-check by having a colleague review the email and attachment to ensure they are correct
- Strictly controlling administrative access to networks and applications. Administrators must use uniquely assigned accounts which are not used for normal business access
- All accounting, payment and procurement systems activity should be logged. This includes online banking. Challenging banks to ensure that they can provide a reliable audit trail of activity should an investigation be needed can prove invaluable
- **Protect the Most Vulnerable**

  Modern fraudsters have well-developed processes which include gathering intelligence about their target victims. These criminals do not want to waste their time and so discovering and targeting those who control or influence payments is an activity of primary importance to them.

  Those staff responsible for functions in finance / accounts, procurement, and benefits are most at risk but even staff involved in areas involving refunds or repayments may also be targeted.

  The first thing to do is to protect these staff by ensuring it is not easy for attackers to identify them specifically. This is not easy for organisations who may be used to promoting openness, but a good place to start is to ensure that contact information is non-specific and not published externally or internally unless it absolutely must be, and even then, only to those on a specific need-to-know basis.

  The third key protection is to implement a process of oversight; the 'double check.' No matter what the process of payment or procurement is, ensure that there is always a dual-control step. In payments, segregate those who can raise from those who can release. In procurement, ensure the use of effective processes of due diligence and authorisation are split between the staff responsible.

- **The Insider Threat**

  The insider threat of fraud is still very real for commercial, charitable and government authorities. Insider attacks may take place over an extended period and are often driven as much by an insider's personal problems as by malice or greed.

The best way to manage the risk of insider threat is again to take the trouble to double check. Where possible, strict due diligence checks should be performed on staff with financially sensitive roles, and warning signs for changed behaviours need to be looked out for. Failure to act in time (or at all) when there are known problems is common in many organisations. Make sure supervision and performance reviews and any subsequent monitoring are performing effectively.

Segregation of duties and strict system access controls should be used as the key operational barriers to prevent fraud. A layer of oversight above this should also mean that any anomalies would be swiftly detected.

Incident reporting and whistleblowing will also serve to enhance legitimate monitoring activities, but they need to be clear, accessible, and destigmatised to encourage staff to use those processes should they have any concerns. Line Managers have a critical enablement role in this respect and should actively promote responsible use of the Authority's reporting channels, leading by example.

- **Lead the Fight**

  It is rare for organisations that have adopted the fraud prevention advice given above to suffer from fraud. Organisations will be more vulnerable if they do not support fraud prevention from the executive level.

  That means appointing an Executive 'Fraud and Cyber Champion' who ensures the assignment of a suitable fraud prevention budget, the appointment of appropriately skilled expertise, and an effective governance framework to monitor and report on incidents and progress improvements.

## Summary

The threat of fraud is constant for all organisations. Whilst it is unlikely that any organisation can manage the risk to zero, there is a great deal of advice and guidance available to organisations to ensure that management systems are robust and can effectively prevent most attempts from being successful.

Significant increases in the cost of living should be recognised by all organisations as a potentially influential factor in increasing the motivation of some individuals to commit fraud, and so should review processes against best practice standards to ensure they have achieved the level of protection to which they aspire.

## Support and Resources

To assess the current level of resilience, we recommend benchmarking against QBE's comprehensive risk controls provided in the following self-assessments:

- Fraud Prevention Questionnaire (part of QBE's Fraud Prevention Toolkit)
- Cyber Risk Profiler

  These are available free of charge to QBE policyholders and are delivered online via QRisk. Both provide detailed guidance notes and a range of template documents, posters, checklists etc. to raise risk awareness and implement controls, and can be requested via qrisk.support@qbe.com

  For a more bespoke approach with the added benefit of expert assistance, QBE policyholders also qualify for discounted assessments with QBE partners STORM Guidance who contributed to the risk management advice in this guidance note. A consultant-guided risk review will provide a jargon-free report advising on further controls needed to improve cyber resilience. This service can be requested direct from STORM - contact@stormguidance.com

## References

1. https://kpmg.com/uk/en/home/insights/2022/01/fraud-barometer.html
2. https://www.ukfinance.org.uk/news-and-insight/blogs/uncovering-the-real-cost-of-fraud
3. https://www.cifas.org.uk/insight/public-affairs-policy/fighting-fraud-corruption-local-authorities/FFCL-Strategy-2020
4. https://www.publicfinance.co.uk/news/2019/01/benefit-assessors-london-councils-convicted-fraud
5. https://www.bbc.co.uk/news/business-55824139

## Further Information

For access to further RMP Resources you may find helpful in reducing your organisation's cost of risk, please access the RMP Resources or RMP Articles pages on our website. To join the debate follow us on our LinkedIn page.

## Get in Touch

For more information, please contact your broker, RMP risk control consultant or account director.

**Risk Management Partners**

The Walbrook Building
25 Walbrook
London EC4N 8AW

020 7204 1800
rmpartners.co.uk

This newsletter does not purport to be comprehensive or to give legal advice. While every effort has been made to ensure accuracy, Risk Management Partners cannot be held liable for any errors, omissions or inaccuracies contained within the document. Readers should not act upon (or refrain from acting upon) information in this document without first taking further specialist or professional advice.

Risk Management Partners Limited is authorised and regulated by the Financial Conduct Authority. Registered office: The Walbrook Building, 25 Walbrook, London EC4N 8AW. Registered in England and Wales. Company no. 2989025.