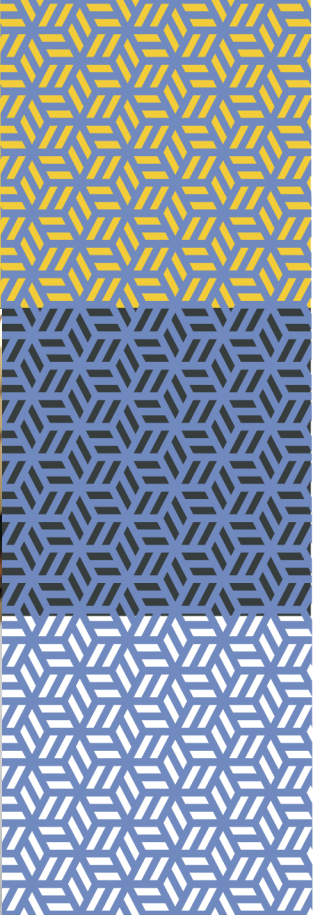
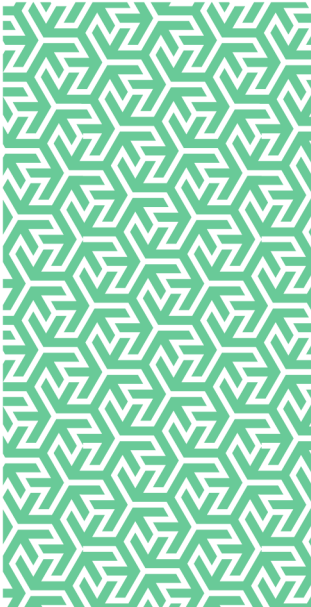


rmp

**Risk control**  
Fidelity & Forgery



In partnership with



**GALLAGHER  
BASSETT**

GUIDE. GUARD. GO BEYOND.



# Fidelity & Forgery

## Introduction

In March 2018, the Accounts Commission published its 'Report on significant fraud'<sup>1</sup> on the audit carried out in 2016/17 within Dundee City Council. The case in question concerned an employee of the Council who was able to embezzle more than £1 million over a seven year period, despite annual audits taking place. The report cites 'failures in fundamental controls within the council allowed this fraud to continue over a prolonged period' and goes on to indicate that *'the extent of the fraud, between August 2009 and May 2016, could have been limited if the local authority had addressed significant weaknesses in its invoicing systems'*.

Whilst this particular case is one of the most recent and has a high value attached to the fraud, it is not isolated. A search on the internet can reveal several cases of differing value involving public, private, and third sector organisations.

## What do we mean by Fraud?

Section 1 of The Fraud Act 2006, broadly defines three main types of fraud:

- 1 Fraud by false representation
- 2 Fraud by wrongfully failing to disclose information
- 3 Fraud by abuse of position.

Fraud can be perpetrated by customer, employee, or a supplier and can take many forms including Procurement Fraud, Travel and Subsistence Fraud, Exploiting Assets and Information, Payment Fraud, Receipt Fraud, and False Accounting. According to UK Finance<sup>2</sup>, in 2017 the financial industry stopped an average of almost £4 million in unauthorised fraud every day.

The management of fraud risk must form part of an organisation's Corporate Governance arrangements which includes effective systems of internal control, including financial, operational and compliance, with a view to the achievement of the Council's priorities/objectives.

## Risk Assessment

Risk taking is an essential part of business in order to progress, grow, produce innovative products and efficient services etc. and the management of that risk is critical to success.

<sup>1</sup> [Audit-Scotland.gov.uk](http://Audit-Scotland.gov.uk)

<sup>2</sup> [UK Finance](http://UK Finance)

Therefore, risk assessment is a keystone of Corporate Governance that helps identify where you may be at risk from fraud, assesses the level of risk, and implements controls to reduce those risks where possible and, stay in control.

Fraud is a threat to an organisation's ability to ensure it manages its financial affairs and during the risk assessment, you will identify proactive controls to prevent and detect it, and reactive controls to respond to suspicions or allegations of fraud.

## Prevention

The first step to carrying out a fraud risk assessment is to identify your vulnerable assets. These include, but are not limited to, buildings, money, and customer data. They are valuable to your organisation. Also consider the potential scale of fraud.

Once you've identified them, you'll need to think about how to reduce the chances of those assets being defrauded or stolen. One strategy would be to identify why they would be of value to someone and how that person may commit fraud.

Internal threats can come in many forms and may include an employee unintentionally allowing others to commit fraud through a lack of information security procedures.

Alternatively, it may be an opportunist employee targeting the employer's assets.

In some cases 'unrestricted access', as in the Dundee City Council case, will provide the opportunity to commit fraud.

### 1 Do you have any employees with unrestricted access to financial systems?

There was an ability to exploit a loophole, sending money to a personal own account while pretending it was going to genuine suppliers.

### 2 Have you made proactive attempts to identify any potential loopholes in your system?

There was a lack of segregation of duties which allowed access to a number of systems, enabling the fraud to be perpetrated.

### 3 Is there a lack of segregation of duties for any employee who has access to financial systems?

Internal controls such as system reconciliations were not carried out, or were ineffective resulting in failure to identify payments as anomalies for further investigation at an early stage.

#### **4 Do you have an effective system of reconciliation which would identify anomalies?**

Next, build controls into your routine business processes. Ways of doing this will vary depending on the business and asset, but will include things like managerial oversight of finance processes, ensuring that one person cannot transfer high value assets by themselves or without sign-off, regular checks and audits of your assets, and restricting access to key assets to only those who need to use them. To prevent fraud there must be an understanding of the causes that allow fraud to occur, and the means by which to carry it out.

### **Preventative Controls**

There are simple things you can do to begin to protect yourself from threats within your business.

#### **Anti-fraud policy statements**

Adopting an anti-fraud policy statement is one way of communicating a strong fraud prevention message to your staff.

Such a statement, endorsed by the head of the organisation, provides a clear understanding that the organisation promotes a zero tolerance culture to fraud.

#### **Pre-employment checks**

Most employers now engage in pre-employment checks and this can be useful in reducing the chances of internal fraud. Always ask for at least two independent references when taking on new staff and verify their personal information and background wherever possible.

#### **Staff behaviour**

Monitoring of employees' performance is standard practice these days and helps understand what makes a person the type of employee they are. It can also unearth internal threats to your organisation. Identifiable behaviours can include a sudden change of lifestyle, unexplained wealth, a reluctance to take a holiday or promotion, or being scornful of systems and controls.

In almost all cases there are simple explanations for these behaviours, but it is sensible managerial practice to be alert to the possibility that those acting out of character could be up to no good. Remember, even long-serving employees could be tempted to commit fraud under certain circumstances, so it is equally as important to watch out for any strange behaviour in those you think you know well.

### **Detection**

Detection is about having a system of checks and balances to ensure things are working as expected.

Many public sector organisations are now employing dedicated Fraud Officers to develop and implement proactive preventative systems, and react to allegations.

All public sector, charities etc. are subject to an external auditing programme and this is one system which may pick up some anomalies in accounting and financial management, however, this can be a general overview rather than in-depth audit. The internal auditing system should be more effective as those carrying out the audit should be aware of the internal working of the financial systems, and other systems which link in to this, and may not be constrained by timescales.

However, as was the case with Dundee City Council, auditing systems were ineffective at identifying the perpetration of fraud.

### **Protection**

Where the results of the risk assessment indicate that there is a potential for fraud on a large scale, there is an option to take out insurance as protection against loss of funds.

Fidelity Guarantee insurance is an insurance policy designed to indemnify the insured (the employer) for the loss of money or property sustained as a direct result of acts of fraud, theft or dishonesty by an employee in the course of employment.

The policy pays the actual financial loss sustained as a result of the dishonesty/ fraudulent act of the employee.

### **Conclusions**

Fraud has the ability to impact upon the organisation's reputation and financial stability and will ultimately affect the achievement of objectives. All Council's should have identified fraud as a risk on their Operational Risk Register, if not their Strategic.

## 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.

[contact@mpartners.co.uk](mailto:contact@mpartners.co.uk)



### **Risk Management Partners**

The Walbrook Building  
25 Walbrook  
London EC4N 8AW

020 7204 1800  
[rmpartners.co.uk](http://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.