PROCUREMENT FRAUD IN THE PUBLIC SECTOR

An Equifax whitepaper
Autumn 2016

EQUIFAX®

Contents

Introduction

Procurement fraud is any fraud relating to an organisation purchasing goods or services from third parties, including the sourcing, letting of contracts and contract management phases of the procurement cycle.

Procurement fraud can happen at any point within a contract lifecycle across both the pre-contract and post-contract phases and can be committed in many ways, including:

- Bid rigging and manipulation of the procurement process
- Collusion between suppliers and / or between staff with the procuring organisation and suppliers
- Creation of 'phantom' companies to commit fraud
- Supply of false invoices, or invoices with unauthorised additional costs
- Staff diverting legitimate payments intended for suppliers to themselves
- Suppliers not supplying the agreed quality and / or good and services.

Public Sector organisations procure a wide range of goods and services, often duplicating the requirements across departments. Significant work has been undertaken by Crown Commercial Services to try and ensure that the procurement regulations are followed. The United Kingdom's impending exit from the European Union will have a marked effect on these procurement regulations, as will the set-up of a new Government Commercial Organisation housed in the Cabinet Office. However, despite these two major changes, at a practical level, where the actual procurement is undertaken, the risks still exist and need to be addressed.

This paper highlights examples of where in the procurement lifecycle there is a risk of fraud, and offers our thoughts on how you can mitigate the risk of it. It provides simple, practical and cost-effective controls that can be implemented, without huge set up costs, but which can make a significant impact on the level of procurement fraud suffered regardless of whether you work in Central Government or Local Government.

The impact of procurement fraud

The impact of procurement fraud is wide-ranging. The true financial cost of any type of fraud is hard to quantify, but according to the Annual Fraud Indicator 2016[1], of the £112 billion spent on procurement by Central Government, the estimated fraud was £5.4 billion. Similarly, within Local Government, of the £86 billion spent on procurement, the estimated fraud was £4.1billion. These figures relate to 4.78% of the total expenditure. If these losses could be reduced then the monies saved could be re-invested in the provision of public services.

However, there are other consequences resulting from procurement fraud than just the financial loss to an organisation, including:

The risk of reputational damage

Resources needed for investigations once potential fraud has been detected, and to take any subsequent legal action

Lower staff morale

Operational impact from the loss of supply of goods and / or services

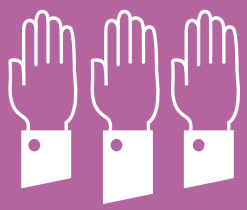
Increased workload in detecting procurement fraud

Procurement fraud: where does it occur?

There is a risk of fraud occurring at each stage of the procurement process, at commencement of the process, i.e. pre-contract award, and then throughout the period of the contract, i.e. during contract management. There is also a risk of procurement fraud even when a Central or Local Government organisation has not procured specific goods or services. If procurement fraud is to be kept to the absolute minimum then Public Sector organisations need to put in place a robust and comprehensive strategy to combat it at each stage.

This strategy should:

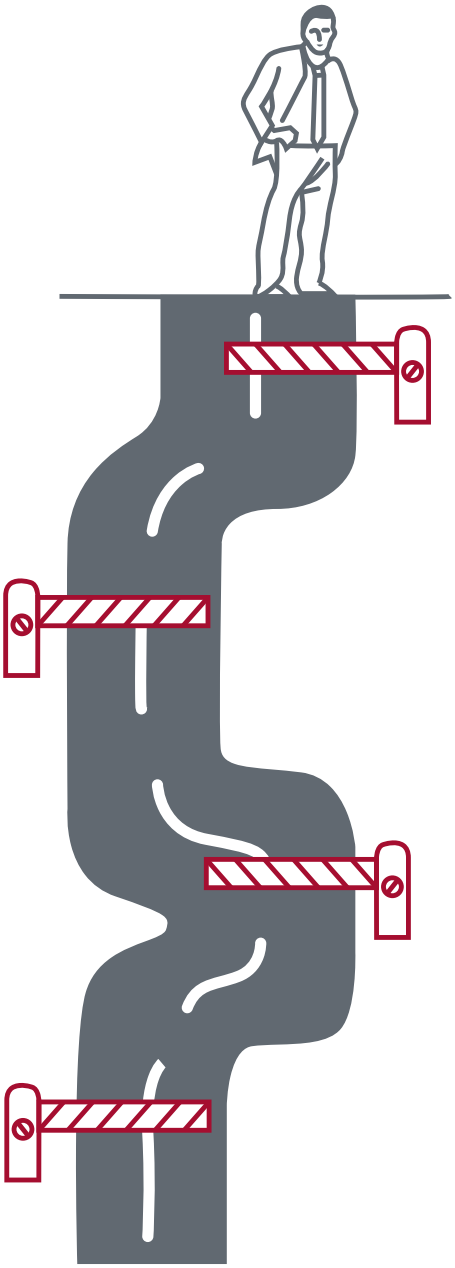
Be 'risk-based', i.e. it should reflect the size and duration of all contracts - checks made for a low-value, short-term contract might be less than those made for a high-value, long-term one;



Have the buy-in of all key stakeholders within your organisation, including the support of management at the highest level;

Be transparent, verified in its application, and fully audited so that a comprehensive record of all checks that were performed is retained for future reference;

Be regularly reviewed to ensure that it remains 'fit for purpose'.



Pre-contract award

Public Sector organisations need to conduct a robust series of checks before contract award. Not only will this help reduce the risk of procurement fraud but it will save time, effort and potentially embarrassing and expensive mistakes later on in the procurement process. Such checks should identify:

- Whether the potential suppliers are genuine and legitimate businesses (to highlight phoenix or shell companies);
- The current financial status of the potential supplier. Note that annual accounts filed by a business are not verified and are not up-to-date, so do not provide a true indication of their financial status;
- Whether there is any link between the potential supplier and any staff members within your organisation that are key decision makers in the procurement process;
- Checks on the legitimacy and financial status of all major subcontractors that the potential supplier intends to use in order to fulfil the contract;
- Anti-money laundering checks
- Whether there is any previously-recorded negative information about the potential supplier, or its key personnel, from other Public / Private Sector organisations, for example on CIFAS, or on another shared database / fraud hub;
- The reputation / public perception of the potential supplier through checks on social media etc.;
- Whether there is any evidence of potential suppliers colluding over the prices that they quote.

Contract management lifecycle

Once the contract has been signed, the contract management phase of the relationship begins. The checks conducted at the pre-contract phase need to be repeated, or updated, as due diligence to ensure that the supplier remains fit for business and has not waited until they have a signed contract to begin fraudulent activity. Other recommended checks include:

- Criminal record checks on key individuals within the supplier's organisation (or subcontractor), particularly if they are to work with you and / or on your premises;
- What is the latest financial status of the supplier / subcontractors? For example, is there any new evidence that they were not a legitimate business, that they are now financially stressed, or that a recent FCA fine[2] has been imposed?
- Is there any new derogatory information about any of the supplier's key personnel, for example being disqualified as a Director, or their name being added to a sanctions list?
- Are the bank account details provided by the supplier for payment genuine, and do they actually belong to the supplier?
- Are invoices sent by the supplier correct, i.e. for the agreed goods or service, for the correct term, and for the agreed amount? Have duplicate invoices been sent?
- Have purchase orders been raised for services or goods that have not actually been procured, or where there is no evidence that a service has been received?
- Are contracts being extended without justification, i.e. has the original contract term ended and the contract automatically renewed without going back to market where a more advantageous contract may be supplied?

Public Sector organisations need to take a proactive approach to these checks as suppliers may not own up to detrimental information at contract review meetings.

'No Contract' procurement fraud

Public Sector organisations can also face the risk of fraud even when they have not engaged in any procurement activity. For example, false invoices can be received for goods and / or services that were never procured, with the fraudster hoping that they will go undetected and be paid. As above, verification of ALL invoices received should be performed prior to payment, and details of any suppliers of false invoices shared with other organisations.

Internal due diligence

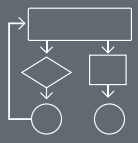
Performing regular due diligence checks on staff will ensure that the risks of internal fraud are greatly reduced. This should cover not only the procurement staff involved in the bid process and award, but the finance staff and all senior managers who could influence others.

Obviously, any irregularities will need to be channelled to the Internal Audit team, but checking for early indications of fraudulent activity, or of those who may be susceptible to coercion to commit procurement fraud (e.g. through being in financial difficulties) could be flagged by due diligence checks which also protect staff from false accusations.

Initiatives to help combat procurement fraud

There have been a number of initiatives to help organisations to combat procurement fraud, including:

There have been moves by Public Sector organisations to establish a culture of fairness, responsibility, accountability, honesty, integrity including zero tolerance of fraud / corruption and to support for whistle blowing



There have also been moves to implement more robust procurement processes such as centralised procurement, fraud training and education, and benchmarking against 'similar' organisations

OCDS

The Open Contracting Data Standard[3] has been created to help reduce costs, create more competitive contracting and prevent fraud and corruption

NAFN

NAFN (www.nafn.gov.uk) exists to help public sector organisations share data and information relating to common frauds, including procurement fraud

Many Local Authorities are helping lead the drive against procurement fraud with the support of the Local Government Association, CIPFA and others through the 'Fighting Fraud Locally[4]' initiative

Invoicing tools can be deployed that look for duplicate invoices / payments

Analytical software packages exist which help organisations to wade through massive amounts of data to help predict, prevent and disrupt all types of fraud.

How we can help you mitigate the risks of procurement fraud?

We leverage our extensive consumer and commercial data assets to derive real insight that helps clients in both the public and private sectors to make informed decisions regarding many aspects of their business operation, including fraud. In order to help organisations establish an efficient and cost-effective strategy for combatting procurement fraud we can provide access to a number of proven services that can be deployed individually, or combined to produce a more comprehensive solution. The diagram below provides an overview of our capabilities:

Milestone: Pre-contract award checks

Risks	Controls
Bid rigging	• Checking of suppliers, looking for directors, (including disqualified directors) and shareholders to see if they are linked to, or live nearby, procurement staff or senior staff who could influence junior staff; • Checking that the supplier is fit to do business with, e.g. identification of adverse data such as CCJs or involvement in any previous fraud; • Confirmation that suppliers bidding are not linked, either by company structure, location or by their directors / shareholders; • Checking sanctions lists for matches to the directors and shareholders of a supplier, as well as of their relatives and close associates.
Creation of shell companies to facilitate fraud	• Checking that suppliers exist, how long they have existed for, that they are actively trading, and what their financial status is; • Confirmation of the directors / shareholders of suppliers to look for evidence of collusion; • Checking for evidence of suspicious activity in the supplier's location, e.g. CCJs at the same postcode, similar names of companies or similar directors.

Risks	Controls
Phantom suppliers	• Checking that suppliers exist and are actively trading; • Checking for evidence of suspicious activity in the supplier's location, e.g. CCJs at the same postcode, similar names of companies or similar directors.
Bank account verification	• Confirmation that the supplied bank account sort code and account number belong to a real account and that they belong to the supplier, and not to an individual • Checking for evidence that the bank account has not been subject to cyber fraud and whether it has been taken over, e.g. the name on the account does not match that of the supplier; • Checking whether the device used to provide the supplier's tender response has been used for fraudulent purposes before.

Milestone: Contract management lifecycle

Risks	Controls
False invoices	• Confirmation that the bank account sort code and account number belong to a real account, and to the supplier, and not to an individual.

Milestone: Internal due diligence

Risks	Controls
Collusion with supplier	• Checking of suppliers, looking for directors, (including disqualified directors) and shareholders to see if they are linked to, or live nearby, procurement staff or senior staff who could influence junior staff; • Checking that the supplier is fit to do business with, e.g. identification of adverse data such as CCJs or involvement in any previous fraud; • Confirmation that suppliers bidding are not linked, either by company structure, location or by their directors / shareholders; • Checking sanctions lists for matches to the directors and shareholders of a supplier, as well as of their relatives and close associates.
Falsifying purchase orders	• Checking whether the 'new' Purchase Order contains different bank account details to those used previously. If so, then verification that the new bank account sort code and account number belong to a real account, and that they belong to the supplier, and not to an individual.
Amending suppliers bank details	• Adherence to strict internal processes when amendments to a supplier's bank details are required, including sign-off and verification that the new bank account sort code and account number belong to a real account, and that they belong to the supplier, and not to an individual.
Risk of blackmail / coercion	• Investigative checking (under Section 29 of the Data Protection Act) of the financial status of staff in key posts, e.g. if they are heavily in debt this might expose them to a higher risk of blackmail or coercion from suppliers; • Income verification of staff in key posts to check if there is an unusually high flow of funds through their bank account, suggesting an additional source of income.

What are the benefits of mitigating the risk of procurement fraud?

In addition to the financial savings that will result from lower levels of procurement fraud, there are many other benefits from mitigating the risk. These include:

- Reputational risks are substantially lowered as appropriate checks are carried out pre- and post-contract award, with a full audit trail of actions taken to provide evidence of what activity was undertaken;
- An increased degree of confidence that the supplier is genuine, is financially stable and is not 'high risk' (e.g. a supplier, or a close relative, is not on a Sanctions List);
- A lower level of risk that the supplier will act fraudulently during the period of the contract (if pre-contract award checks are carried out);
- Less chance of a supplier going bankrupt and defaulting on a contract if appropriate financial checks are carried out prior to contract award, and subsequently via ongoing monitoring;
- Protection against staff fraud, and accusations of such fraud, due to regular due diligence checks being carried out;
- A reduced risk of paying an incorrect or fraudulent supplier when bank account verification is carried out on a regular basis, and always when a request is received to amend the bank account details on a purchase order.

Finding out more

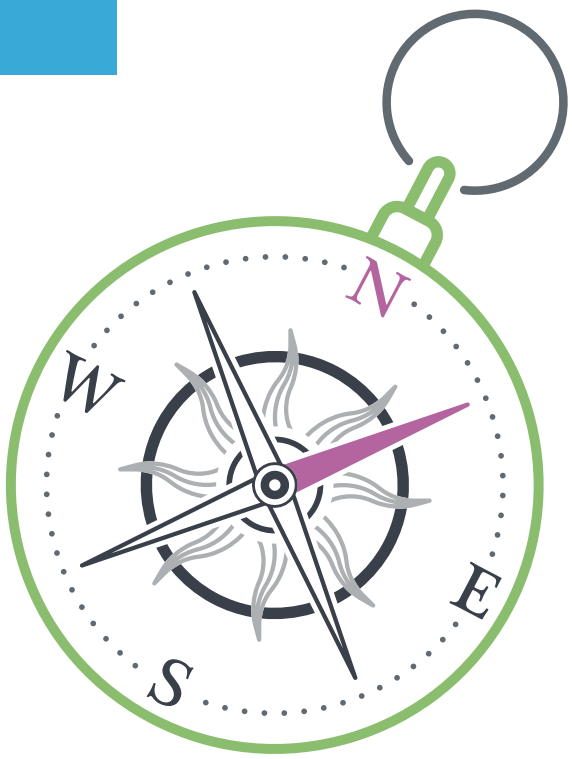
We would be pleased to provide further details of how we can help Central and Local Government mitigate the risk of procurement fraud. In order for us to do so, please contact:

For Central Government and Enforcement please contact Julie Hewitt, Account Director, Central Government

Julie has worked with Central Government over the past two year helping them to tackle fraud, error and debt, as well as identity verification, commercial investigations and credit applications. Her knowledge is based on 18 years' experience of working in Central Government. She has qualifications in Information Security and in Purchasing and Supply (CIPS).

For Local Government please contact Sarah Oliver, Business Development Manager, Local Government

Sarah has worked with Local Authorities in various industries for the past 17 years, with the last 4 years being with Equifax. Sarah's experience covers numerous departments within a Local Authority, where she has always taken a collaborative approach to gaining a deep understanding and solving, of the many challenges Local Government face, in an ever changing landscape.



Sources:

1 Annual Fraud Indicator 2016, University of Portsmouth Centre for Counter Fraud Studies, 2016, http://www.port.ac.uk/media/contacts-and-departments/icjs/ccfs/Annual-Fraud-Indicator-2016.pdf
2 https://www.fca.org.uk/firms/fines-%E2%80%93-2016
3 http://www.open-contracting.org/data-standard/
4 https://www.gov.uk/government/publications/fighting-fraud-and-corruption-locally-2016-to-2019

All links correct as at September 2016

To contact Julie Hewitt or Sarah Oliver please call us on 0800 085 4156 or email ukmarketing@equifax.com

EQUIFAX®