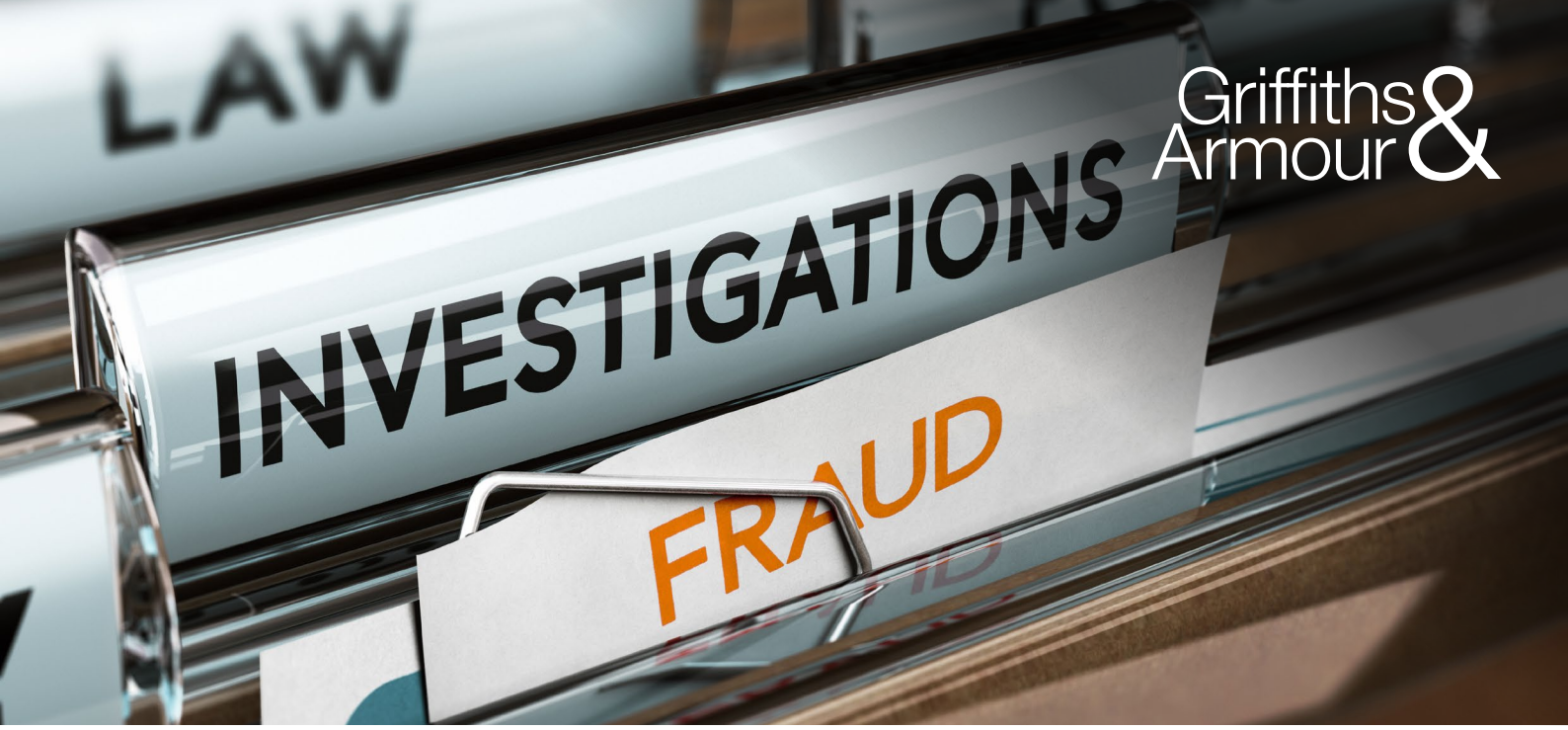
Griffiths & Armour

FRAUD

RISK DIRECTORY 2020/2021



Griffiths & Armour

FRAUD
RISK DIRECTORY 2020/2021
INTRODUCTION

Despite difficulties in arriving at an accurate figure due to suspected under-reporting, a recent study estimated that fraud losses in the UK could total as much as £190 million each year. Furthermore, since 2009 such losses have reportedly risen by over 50%. In the wake of these statistics and following several high-profile cases, many organisations are increasingly becoming aware of the need to have specific fraud risk management procedures in place.

Fraud can take many forms. It can be perpetrated by an individual or several parties, i.e. collusion. It can originate external to an organisation, within it or be a combination of both.

Some brief examples of different types of fraud are provided below:

- Misdirection of money or acquisition of goods, for example via fake emails, forged documentation and/or telephone call deception, commonly referred to as 'social engineering'.
- Payment fraud, for example using stolen or cloned payment card details.
- Internal misappropriation of money and assets, for example via embezzlement or theft.
- Revenue or assets gained by fraudulent or illegal acts, for example, over-billing customers.
- Expenses or liabilities avoided by fraudulent or illegal acts.
- Fraudulent financial reporting, for example, understatement of liabilities.

This guidance seeks to provide an overview of the primary legislation in this area and outline general fraud risk management practices. Please note that the risk of bribery, corruption, tax evasion and money laundering are not within the intended scope of this document.

KEY LEGISLATION

There are several areas of legislation that cover fraud, however, the primary areas of legislation are considered to be the Fraud Act 2006 and the Theft Act 1968. An overview of this legislation is detailed below:

FRAUD ACT 2006

The Act provides for a general offence of fraud and specifies the three ways in which it can be committed. For each, a prerequisite is that the behaviour must be dishonest and intended to secure a gain for the fraudster or a loss to another. The three ways in which the general offence can be committed are:

False Representation For a representation to be false, it must be wrong or misleading, and the person making it must know that it is, or that it might be.

Failure to Disclose Information This offence applies where an individual fails to disclose information to another where there is a legal duty to do so.

Abuse of Position This would apply where an individual, expected to safeguard the financial interests of another, abuses their position. The offence can be committed by either an act or omission.

The Act also contains several other fraud offences and these include:

- Possessing articles (including electronic data or programs) for use in fraud.
- Knowingly making or supplying articles for use in fraud.
- Fraudulent trading of businesses not covered by a similar offence under Section 993 of the Companies Act 2006. Such businesses include sole traders, partnerships, trusts and companies that are registered overseas.
- Obtaining services dishonestly.

It is important to note that the Fraud Act 2006 does not apply in Scotland where fraud is mainly dealt with under common law and a variety of statutory offences in specific areas.

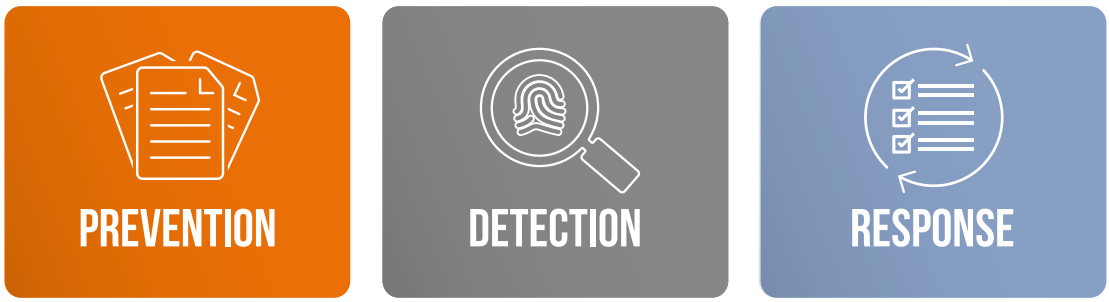
THEFT ACT 1968

This legislation includes the offences of false accounting and false statements by company directors.

Aside from legislation, civil remedies are also available for fraud, such as via the tort of deceit.

FRAUD RISK MANAGEMENT

Fraud risk management can be summarised under three main headings:



These are now considered in more detail.

PREVENTION

It is always preferable to avoid fraud and therefore prevention control measures are considered particularly important. Areas to address include:

- Fraud Policy.
- Risk assessment.
- Control measures.

FRAUD POLICY

A Fraud Policy and/or Employee Code of Conduct should be endorsed at the most senior level and give a clear indication of the organisation's position on fraud and its expectations of staff. Areas to consider for inclusion in a Fraud Policy include a statement on ethical values and a commitment by the orgainsation to:

- Take appropriate measures to deter fraud.
- Introduce and maintain necessary procedures to detect fraud.
- Encourage employees to report any potential suspicion of fraud.
- Investigate all instances of suspected fraud.
- Report any incidences of suspected fraud to the appropriate authorities.
- Assist the Police in the investigation of any suspected fraudsters and any subsequent prosecution.
- Recover wrongfully obtained assets and money from fraudsters.

RISK ASSESSMENT

A fraud risk assessment can assist in identifying higher risk areas or weaknesses in current controls. Areas to focus upon include:

- Product and service outputs.
- Customer and supplier
- Revenue generation records (in particular bank account, address and contact details).
- Revenue collection and control.
- Refunds.
- Expenditure
- Suppliers and inputs.
- Asset utilisation, acquisition and disposal.

CONTROL MEASURES

Specific controls and procedures should be implemented for any higher risk activities as identified by the risk assessment. In addition, the following is also considered good practice:

- Considering fraud control measures as part of any planned changes to operations and activities. In higher risk areas changes should ideally be subject to a suitable authorisation procedure.
- Defining clear responsibilities, levels of authority and reporting lines for individuals.
- Segregating duties and/or rotating staff in higher risk areas.
- Structuring responsibilities such that undue reliance is not placed upon any one individual, including those in senior positions.
- Requiring employees to advise the organisation of any potential conflict of interest.

- Requiring proof of identity and/or original supporting documentation, such as receipts and invoices, before authorising payments or providing goods or services.
- Independently validating any requested change of bank account, delivery address or contact details prior to amending records.
- Organising systems and procedures to facilitate a full and secure audit trail.
- Including sequential numbering on key documentation to reduce the risk of unauthorised copying or counterfeiting.
- Exercising due care and attention when engaging individuals or organisations, commensurate with the potential for them to commit fraud. Additional vetting may be considered appropriate in higher risk instances. This can include information on:
  - General history.
  - Character references.
  - Financial propriety.
  - Criminal record.
- Verifying the identity of customers.
- Ensuring that appropriate security measures are established for assets, sensitive information, intellectual property, financial stationery, IT and payment systems. Reference should be made to security standards for IT and payment systems, such as ISO 27001, Cyber Essentials and PCISS (Payment Card Industry Security Standard).
- Introducing asset registers and asset marking.
- Maintaining an approved suppliers list.
- Providing training and information for all staff. This can promote a higher awareness of fraud risks and the control measures already in place. It can also deter those who might otherwise consider committing fraud.

DETECTION

Detection regimes form an essential part of any fraud risk management strategy. Examples include:

- General monitoring and supervision.
- Conducting audits.
- Investigating potential fraud indicators.
- Data analysis.
- Whistleblowing.

These are now considered in turn.

GENERAL MONITORING AND SUPERVISION

This should be integral to the day-to-day operations of an organisation and focus upon key risk areas as identified by the fraud risk assessment. Examples can include internal financial reporting and budgetary controls. Consideration should also be given to undertaking random spot checks in various areas, such as taking asset inventories.

CONDUCTING AUDITS

Audits determine whether existing control measures are effective and can be either undertaken in-house, for example by an audit committee, or by an independent third party, such as an organisation's financial auditors. It is recommended that these be conducted periodically to repeatedly test how robust an organisation's practices are against fraud. Dependent upon the risks presented, consideration should also be given to auditing key third parties.

INVESTIGATING POTENTIAL FRAUD INDICATORS

Examples of potential fraud indicators include:

- Unusual employee behaviour, for example: reluctance to take leave; refusal of promotion; mundane tasks retained rather than delegated; over dedication to a particular role; unexplained wealth; new staff resigning quickly and staff appearing stressed without cause.
- Management frequently over-riding internal controls.
- Overly complicated answers given to routine enquiries.
- Key documents going missing, for example, invoices, contracts, etc.
- Continual variations to budgets or contracts.
- Financial checks that cannot be balanced.
- Regular and/or long-standing accounts queries or customer complaints.
- Excessive movements of cash or transactions between accounts.
- Duplicate payments.
- 'Ghost' employee or customer records.
- Staff, customers or suppliers insisting on dealing with only one individual.
- P.O. box numbers as shipping addresses.
- Lowest tenders passed over with minimal explanation recorded.

DATA ANALYSIS

Otherwise referred to as 'data mining' or 'data matching', this can proactively identify unusual or hidden relationships between various information or data. This can prove extremely useful in uncovering fraudulent activity, though due consideration should be given to any issues relating to data protection.

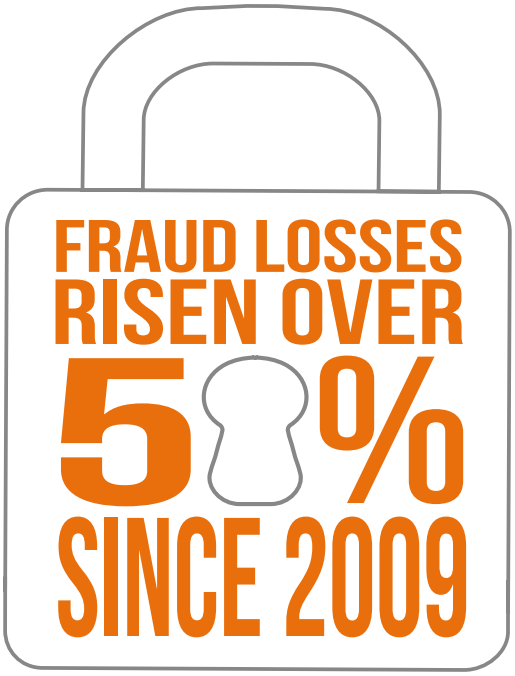
WHISTLEBLOWING

A procedure should be established to allow individuals to confidentially and anonymously raise concerns about fraud.

RESPONSE

It is recommended that organisations establish a fraud response plan. Aspects to be considered as part of such a plan include:

- Instructions on the action required when the suspected fraud is first discovered.
- The reporting line for suspected fraud. As a suspect may be innocent, ideally this should be on a 'need to know basis'. Such an approach may also prevent warning other potentially guilty parties.
- How the suspected fraud will be investigated. Any investigation will need to be undertaken as a priority to allow for necessary changes to be made to prevent a recurrence.
- Securing evidence without alerting suspects to the investigation. Evidence is likely to be easier to collect in such instances.
- Obtaining evidence in a legally admissible form, for example, no marks should be made on original documents and records should be maintained of those having access to evidence.
- Dealing with any employees under suspicion. It is recommended that investigations and subsequent actions be undertaken in conjunction with the human resources department. Consideration should also be given to surveillance arrangements for those under suspicion who are allowed to remain on the premises and searching a suspect's work area and records.
- The procedure for interviewing suspects. It is suggested that the decision to conduct interviews in-house be carefully considered as, if the Police are to be involved, they must be advised at an early stage. In addition, interviews should be arranged such that any statements taken will be admissible in court.
- Guidance on where Police involvement may be considered necessary.
- Tracing and recovering assets.
- Important contacts, such as your insurance broker, accountants, solicitors, etc.
- Potential damage to the organisation's reputation should the fraud become public knowledge. Upon request, Griffiths & Armour can provide guidance on crisis communications.



GRIFFITHS & ARMOUR RISK MANAGEMENT SERVICES

Risk management is a cornerstone of Griffiths & Armour's proposition. Simply put, good quality risk management practices lead to fewer incidents and claims, which in turn help minimise premium spend and retained costs. Our guiding principles for risk management are innovation, practicality and focus on your desired end result, which can be anything from premium reduction to legal compliance. This, coupled with our core belief that you should get the very best we have on offer from day one, ensures a strong partnership based on communication, trust and transparency. Specialisms include:

- STRATEGIC RISKS
- BUSINESS CONTINUITY AND SUPPLY CHAIN
- CYBER RISKS
- ONLINE RISK MANAGEMENT SYSTEMS
- LIABILITY CLAIMS DEFENSIBILITY
- HEALTH, SAFETY AND ENVIRONMENT
- MOTOR FLEET RISK MANAGEMENT
- PROPERTY RISKS

If you would like to discuss any of these risk management services please contact us on 0151 236 5656 or by **email**.

ACKNOWLEDGEMENTS, REFERENCES AND RECOMMENDED FURTHER READING

- The Fraud Advisory Panel Website
- Information Technology. Security Techniques. Information Security Management Systems. Requirements - ISO 27001 - British Standards
- Information Technology. Security Techniques. Code of Practice for Information Security Management - ISO 27002 - British Standards
- Secure Destruction of Confidential Material: Code of Practice - BS EN 15713 - British Standards

LEGAL NOTICE

Insurance Brokers and Professional Risks are divisions of Griffiths & Armour, a partnership which is authorised and regulated by the Financial Conduct Authority.

Risk management services are not regulated by the Financial Conduct Authority.

This document does not provide legal advice and is not a substitute for obtaining specific legal advice in order to protect the interest of your business. Should you require legal advice on any of these matters, please contact your legal adviser. It is intended only to highlight issues that might be of interest to Griffiths & Armour clients. The contents of this document are based primarily on the legal position under English law and may be subject to change. Further, more detailed advice may be appropriate in relation to other jurisdictions in which you work. Where links to third party websites are provided, we accept no responsibility for their content.

Griffiths & Armour

OUR VALUES:

SUPPORTIVE

PERSONAL

PROACTIVE

RELIABLE

& that's the difference

griffithsandarmour.com

Assurex GLOBAL

Insurance Brokers Chartered

IB0223