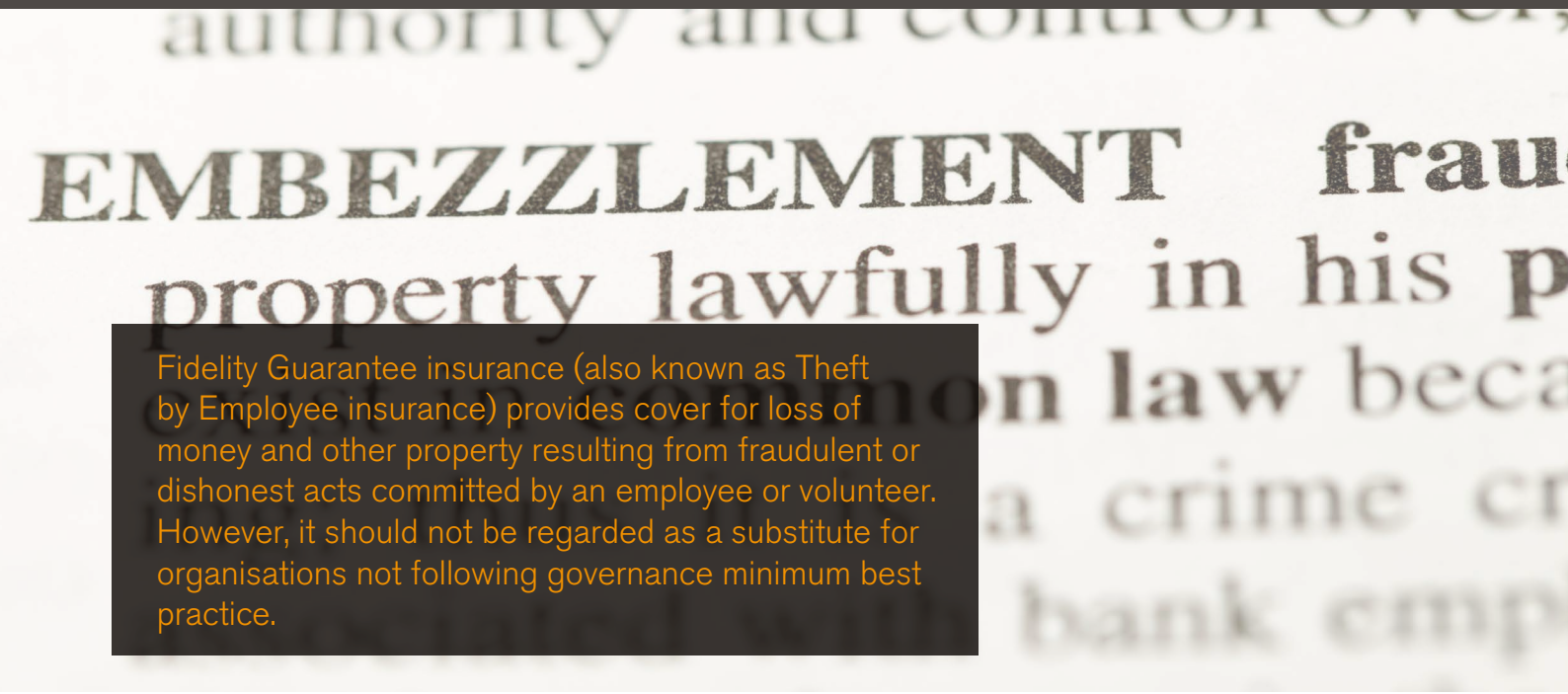
Fidelity Guarantee guidance note



Fidelity Guarantee insurance (also known as Theft by Employee insurance) provides cover for loss of money and other property resulting from fraudulent or dishonest acts committed by an employee or volunteer. However, it should not be regarded as a substitute for organisations not following governance minimum best practice.

Important Note – It is essential policyholders familiarise themselves with the terms, conditions, and Minimum Standard of Control set out in their policy. Failure to comply with these conditions may prejudice their insurance cover and may result in their claim being declined.

Smaller organisations with limited people and resources may not be able to meet minimum insurance requirements or may simply not have the budget to buy this type of insurance. Whether insurance is in force or not, this guidance is intended to highlight minimum best practice in this area to help reduce the risk of losses occurring.

Further questions on this subject should be addressed to your insurance advisor or insurer.

Many organisations take the view that these acts only happen to a small number of organisations and that "it will never happen to them". However, the 2018 KPMG UK Fraud Barometer survey identified the following:

- 10% of UK fraud losses were theft by employee related.
- 60% of fraud losses were committed by management or employees.

Research published by the Charity Commission in 2019 highlighted that:

- 21% of charities believe they are most vulnerable to internal fraud.
- Where identified, fraudsters comprised: 20% paid staff, 18% volunteers and 10% trustees.
- The most common type of fraud was mandate or CEO fraud at 18% followed by abuse of position at 12%.

There are many reasons people commit fraud: for personal gain, in desperation (e.g. a child needs expensive medical treatment), under coercion from organised crime gangs, etc. Sometimes staff in organisations have suspicions or evidence about a colleague's fraudulent behaviour, but feel hesitant about raising concerns. In many cases, organisations may have trusted employees too much.

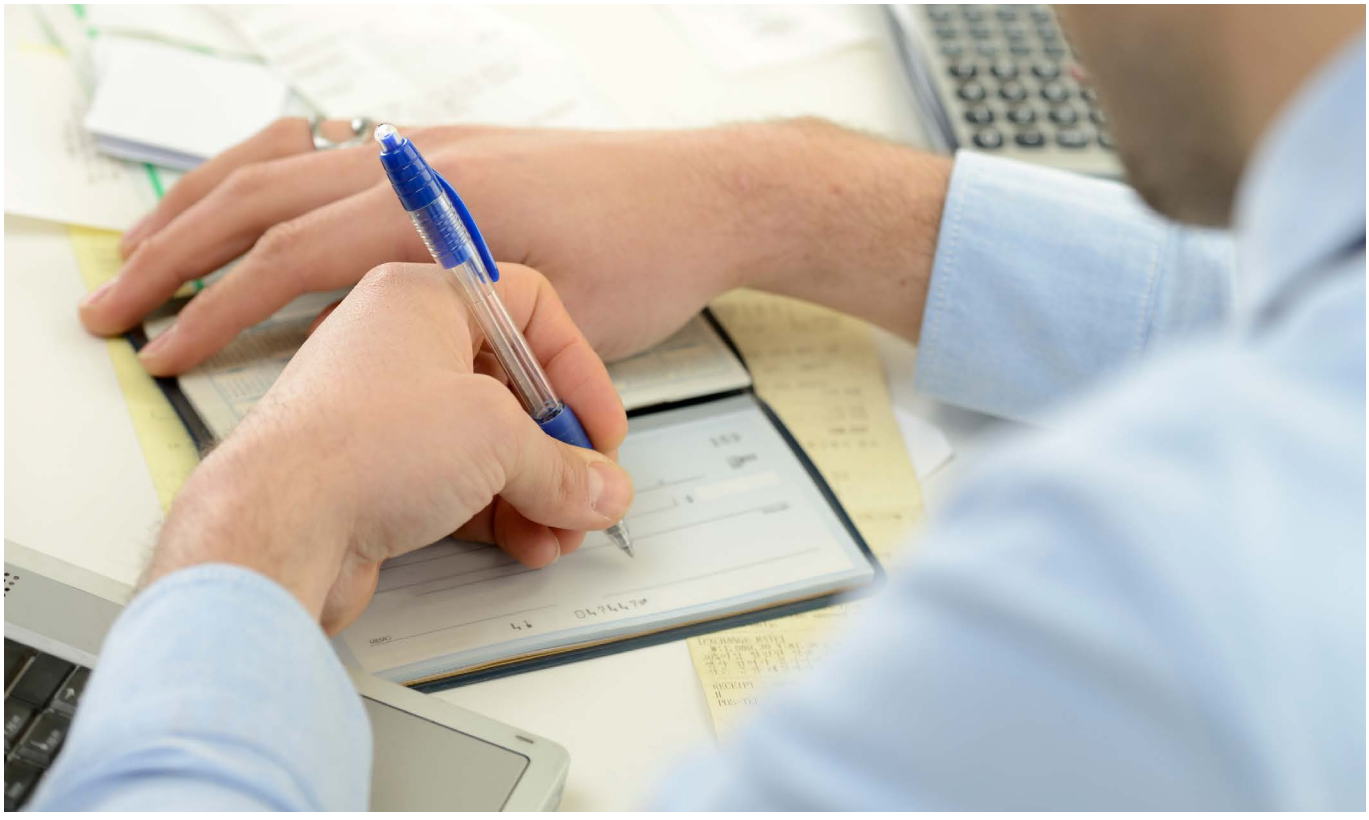
It is very important to be proactive about employee and volunteer theft and implement robust controls. This reduces the risk of this type of theft occurring within your organisation. The time taken and costs in resolving employee theft can significantly impact reputation / brand strength and confidence in the organisation by customers and suppliers. In addition, it can affect staff morale and regulator relationships.

Preliminary Research undertaken by Ecclesiastical highlights real life examples of recent fraud crime.

Amount	Details
£910,000	Finance manager stole money over seven-year period.
£850,000	Charity volunteer treasurer stole money over six-year period.
£550,000	Charity worker transferred money into own bank account.
£300,000	Charity treasurer enabled a gift aid fraud.
£240,000	Long serving finance officer stole from stately home.
£180,000	School CEO used company credit cards for personal use & diverted funds to a shadow company following the sale of school assets.
£172,000	Finance manager of Social Interest Group transferred money to repay money defrauded from previous employer.
£95,000	Commercial Manager stole money to fund gambling addiction.
£70,000	Treasurer stole from their church.
£20,000	PA stole funds to fund holidays and shopping sprees.

Some examples of employee fraud and theft include:

1. Stealing cash, equipment or materials.
2. Creating false payment requests via forged authorisations.
3. Adjusting the amounts on cheques or duplicating cheques.
4. Developing bogus customers or suppliers / non-existent companies and creating false transactions.
5. Stealing passwords to accounts / payment systems.
6. Submitting inflated or false expenses claims.
7. Paying bonuses when they should not have been received.
8. Recording fictitious payments to cover thefts of money or not recording genuine cash receipts.
9. Arranging for mail, invoices or payments to be redirected to different address to cover up thefts.



There are numerous more examples……

Many employees become aware of the strengths and weaknesses in an organisations accounting and systems security. Employees are often more aware of any blind spots and loopholes than more senior management. Most large losses occur when employees steal small amounts of money over a long period of time that aggregates up to a very significant loss to an organisation.

It is essential that minimum best practice includes creating an organisational culture and systems that encourage employees to be proactively vigilant of the potential for employee theft.

Possible indicators of employee theft include the following:-

1. Employees Behaviour

- Unwilling to take time off for annual leave - when others may discover the theft / fraud.
- Late, excessive or unusual working patterns or lone working.
- Employees volunteering for additional responsibilities to gain access financial data or systems.
- Living a lifestyle that appears way beyond their salary.
- Senior colleagues who retain routine tasks outside their role status and requirements.
- Someone with alcohol, drug or gambling addictions.
- Delays in routine financial reports being issued or completion of annual external audits.

2. Adverse Financial Processes

- Holding significant petty cash funds without justification.
- Inconsistencies in accounting information.
- Incomplete invoices or documentation.
- Discrepancies in reporting documentation and bank statements.
- Overdue payments to contractors and customers.
- Lack of invoices, receipts or purchase orders from suppliers.
- Regular shortages of petty cash or supplies.
- Irregular trends in bank deposit statements.

There are many proactive actions to take to make an organisation more resilient from employee theft. It is important to review your financial controls on regular basis to guard against being vulnerable to these type of losses.

Risk Reduction Actions

People

- Obtain written references and always check references with the previous employer / educational experience through a telephone call to validate accuracy.
- Screen new / existing employees by undertaking criminal & financial checks. Create a rolling programme to ensure regular review.
- Retain references & reference check records (in accordance with data protection guidelines).
- For agency workers ensure the employment agency completes adequate checks and carries adequate insurance cover.
- Creating a working environment where employees or volunteers feel valued will make them think strongly before engaging in fraudulent activity.
- Maintain a code of conduct with a zero tolerance towards fraudulent actions. Remind staff of this code on a regular basis asking them to sign up to understanding and acceptance annually.
- Your fraud management policy should advise all cases will be prosecuted.
- Encourage an observant culture, e.g. look for behavioural changes in staff or unexpected extravagant lifestyles.
- Do not encourage lone working.
- Deliver regular training to new and existing staff on financial crime and prevention.
- Create a reporting system – encourage staff to report suspicious activity and include an anonymous whistleblowing email / hotline.
- Require finance staff to take their annual leave including at least 14 days consecutive holiday. Resistance should raise suspicions. Independent checks should be undertaken during this period to check for unusual activity and that record keeping is accurate.
- Enforce regular working hours & do not allow financial staff access to work systems remotely without adequate system security and full audit trails.
- Ensure a ‘clean desk’ policy with confidential documentation locked away when not in use.

Procedure

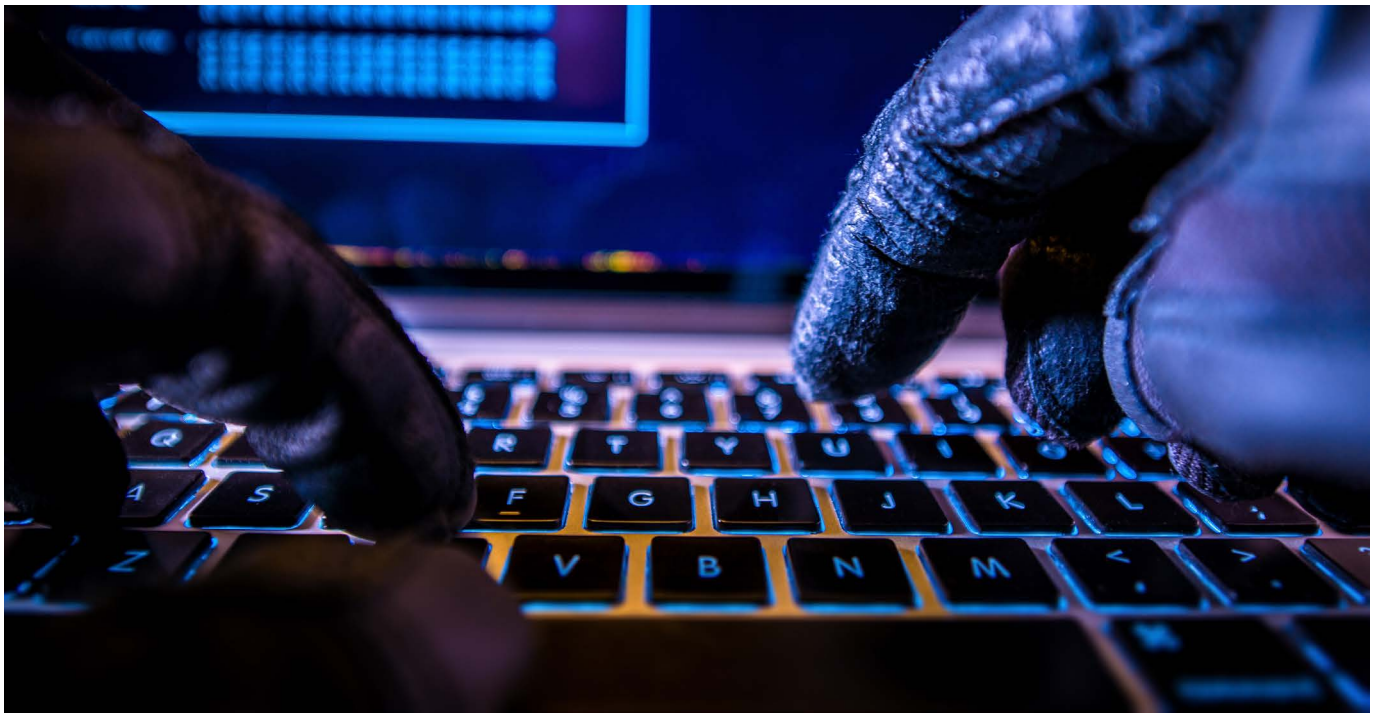
- Financial processes should include separation of duties e.g.
  - Always follow your banks security and controls for any electronic banking.
  - Reconcile accounts independently from staff undertaking day to day accounting duties.
  - Use different employees to enter money payments received into your accounting system to those who actually received the money.
  - Payments to 3rd parties should not be raised, authorised or processed by the same person.
  - Use two-signature controls for payments above an agreed limit and to be signed only when supporting / validating documentation provided.
  - Blank cheques to be securely stored and have restricted access.
  - Regularly review bank statements and on-line banking transactions on a planned and unplanned (spot check) basis.
  - Use an escalating expense sign off procedure.
  - Eliminate petty cash if possible. Many small thefts develop into larger thefts.
- Conduct regular internal checks / audits to ensure prevention measures are being followed and record findings.
- Enable IT systems to incorporate security precautions to monitor transactions and check that staff follow financial procedures.
- Ensure Finance staff personal computer passwords are kept secure, are not shared & require changing on a frequent basis.
- Regular financial reporting procedures and structure should be created that updates the Leadership team and Directors on financial performance.
- A fraud policy should include a fraud response plan.

External Audit

- Use accredited external auditors to formally report on an at least an annual basis. It is important not to just rely on this audit to give reassurance. This audit forms part of your overall control measures, and although this may not always identify internal fraudulent activity it will act as an additional deterrent. It should support other robust internal controls as indicated above.

Cyber Attacks

Cyber crime by external hackers / fraudsters (who are not employees) is rising significantly and this will not be insured by fidelity guarantee insurance. You should additionally consider Cyber Insurance cover. Ensure you follow minimum best practice cyber measures developed by the Communications Electronic Security Group the information security unit of the UK Government.



Conclusion

It is very important organisations understand they can be vulnerable to internal fraud. Essential measures to reduce the risk from this include the following:-

- Proactive whistleblowing policies.
- Awareness training in identifying and reporting fraud.
- Adequate reporting procedures.
- Effective fraud protection measures.
- Regular reviews of fraud controls to ensure they stay fit for purpose.

By undertaking proportionate actions, organisations can reduce the threat of dishonest or fraudulent acts committed by employees and volunteers.

Further Reading

1. Fraud Risk Management – A guide to good practice - Chartered Institute of Management Accountants.
2. Fighting Fraud & Corruption Locally – The Local Government Counter Fraud and Corruption Strategy – CIPFA Counter Fraud Centre.
3. Preventing Charity Fraud – Insights+Action-October 2019. Charity Commission for England and Wales.
4. Fraud Barometer 2018 – A snapshot of Fraud in the UK- January 2019- KPMG LLP.

ecclesiastical

PD3431 1 03/21