PROFiT
Prevention of Fraud in Travel

THE COUNTER FRAUD CAMPAIGN 2019

PART 3: EMPLOYEE FRAUD

Prevention of Fraud in Travel (PROFiT) and the Fraud Intelligence Network (FIN) are working with the City of London Police to reduce fraud in the travel industry. In PART 3 we look the most common frauds committed by employees and list some tips on how to reduce the risks.

PROFiT is the only official travel industry counter fraud body. We work on your behalf to carry out analysis and research, disseminate best practice and disrupt crime.

Find out how you can join the fight against crime. Contact via: contactus@profit.uk.com

1.0 BACKGROUND

Fraud disproportionately affects small companies, says a report by the Association of Certified Fraud Examiners (ACFE). The 2016 Report to the Nations on Occupational Fraud and Abuse concluded that businesses with fewer than 100 employees have the highest number of fraud cases.

2.0 CORRUPTION

2.1 Every organisation is vulnerable to fraud and corruption from existing employees and should have systems in place to reduce the risks.

2.2 Section 7 of the **Bribery Act 2010** creates the "broad and innovatory offence" of the failure of commercial organisations to prevent bribery on their behalf. This applies to all commercial organisations which have business in the UK. Unlike corporate manslaughter, this does not only apply to the organisation itself; individuals and employees may also be found guilty. The offence is one of strict liability, with no need to prove any kind of intention or positive action. It is also one of vicarious liability; a commercial organisation can be guilty of the offence if the bribery is carried out by an employee, an agent, a subsidiary, or another third-party, as found in Section 8. The location of the third-party is irrelevant to the prosecution.

2.3 The crime of a commercial organisation failing to prevent bribery is punishable by an unlimited fine. In addition, a convicted individual or organisation may be subject to a confiscation order under the Proceeds of Crime Act 2002, while a company director who is convicted may be disqualified under the Company Directors Disqualification Act 1986.

2.4 The generally accepted best method of managing bribery risks is for an organisation to take a risk-based approach. The measures taken should be proportionate to the risks faced but you need to keep in mind that no policy or procedure can detect or prevent bribery; they will help focus the effort where it is most needed. There are five steps involved in a risk-based approach:

- Identify the risks you face,
- Assess the risks you face,
- Design and implement systems and controls to mitigate those risks,
- Monitor your systems, and
- Keep a record of what you have done and why you have done it.

2.5 Common risk factors for bribery include:

- The geographical reach of your business – do you operate in companies where there is a high level of bribery and corruption?
- The sectors that you operate in – do you operate in sector that is a high risk of bribery?

Operational risks include;

- Local laws and customs – are there factors which conflict with the Bribery Act 2010?

- Facilitation payments – these are illegal under the Bribery Act 2010
- Gifts and hospitality – could these be construed as a bribe?
- Intermediary relationships – are you due diligence procedures and contractual terms adequate?
- Charitable and political donations – could these be construed as a bribe?

2.6 As a business evolves and its market develops then the bribery risks it faces could change and so risk assessments should be carried out as new challenge or opportunity arises.

3.0 ASSET MISAPPROPRIATION

3.1 Asset misappropriation is a broad term that describes a vast number of employee fraud schemes. In simple terms it is the theft of company assets by an employee. Some examples of asset misappropriation which you might see include where an employee:

- alters the name on a cheque so that it is payable to him/her or a third party;
- alters the payee on a cheque or writes unauthorised cheques;
- steals product from the company, either by taking it or diverting it in some other way;
- steals money;
- skimming (not registering a sale and pocketing the money);
- refund fraud (an employee colludes with someone to return product fraudulently for a refund)
- misuses company services or company funded services;
- sells company product to customers pocketing the money but does not process the booking or funds through company systems;
- provides friends or third parties with company products by-passing the company systems (to satisfy a debt perhaps);
- forges receipts;
- double claims for expenses;
- submits false reimbursement claims;
- inflates expenses claims;
- uses a company expense account for personal expenses and submits them as business expenses;
- uses a company credit card for personal expenses and claims it's a business expense;
- uses a work phone to make premium rate calls;
- over-ordering product returning some and pocketing the refund;
- setting-up a phantom vendor account into which are paid fraudulent invoices;
- initiating the purchase of goods or services on the company for personal use;
- creating false customer accounts to generate false payments;
- discovering that a customer has made a claim against their insurance or credit card, refunds the same amount to themselves or a confederate and changing the customer record to show that the company has paid the customer;
- self-authorising payments;
- colludes with others to process false claims for benefits or payments;
- creates bogus customer accounts in order to generate false payments;
- colluding with healthcare providers in order to defraud an insurance company by submitting false or inflated claims;
- claims reimbursement for health or medical services never required;
- exaggerates or invents disabilities, injuries or medical conditions in order to fraudulently receive compensation;
- attributes to employment injuries or medical conditions caused outside of work in order to fraudulently receive compensation;
- lies about health or work status in order to receive compensation;
- signs off as sick to allow them to take up third a party employment;
- inflates or falsifies sales figures in order to receive higher unearned commission;
- colludes with customers to record and collect commission that is not earned;
- uses a company vehicle for unauthorised personal use;

- uses a company issued credit card for fuel for their own private vehicle and claiming it was for the company vehicle; and
- exaggerates the mileage driven when claiming mileage allowance.

DEALING WITH ASSET MISAPPROPRIATION

3.2 An adage states that, "if you remove the opportunity; you remove the temptation". To reduce the risks of employees committing fraud, staff should only ever have access to systems and financial arrangements that they require to undertake their role. All requests for payment and claims should be supported by evidence such as order forms, invoices and receipts. Additionally, the payment system should be cross referenced the booking or ordering systems so that anomalies can be identified.

3.3 The further steps that companies can take to reduce the risk include:

- Proper management scrutiny of subordinate's work;
- Implement checks and balances;
- Conducting random audits of company accounts;
- Only paying commission once goods and services are delivered;
- Separate work functions so that those who make payments do not also have the ability to authorise payments themselves or make refunds;
- Rotate employees in finance teams' duties;
- Keep chequebooks, company credit cards, and other methods of payment locked away when not in use;
- Take an interest in your employees so that you notice if they begin living beyond their means; such as taking repeated or fancy holidays, or buying a car or house beyond their income;
- Take an interest in your employees so that you can identify if they begin gambling or drinking to excess or develop a drug habit; and
- Implement an anonymous ethics hotline to encourage employees to report wrongdoing.

4.0 ACCOUNTING FRAUD

4.1 An employee who manipulates a company's accounts to cover up theft or uses the company's accounts payable and receivable to steal commits accounting fraud. Employees involved in these types of fraud are generally those in positions that have access to a company's accounts with little or no oversight. Accounting fraud includes:

- Creating false invoices for products or services that were not delivered.
- Colluding with a third party, passing invoices through an account or company the employee controls and taking a cut of the payment in what's known as a "pass-through scheme"
- Initiating purchase orders and payments for goods or services for personal use.
- Setting up a fake vendor account and creating false invoices which are paid to the employee.
- Processing duplicate payments to a vendor, and when the duplicate is returned from the vendor, the employee keeps it. Or processing duplicate payments to create a credit with the vendor then keeping the vendor's next payment.
- An employee sets up a fake supplier and bills the company for goods and services not provided.
- An employee sets up an intermediary company which trades with a legitimate supplier but charges the organisation an inflated sum and skims the excess off into their own account.
- An employee uses company funds to pay for personal goods and services and records the purchases as legitimate business expenses in the accounting system.
- An employee pays an invoice and then makes a second payment to themselves but records it as a disbursement in the accounting system as a payment to the same supplier.
- 'Lapping' (or robbing Peter to pay Paul); where a person in the accounts receivable team pockets a payment themselves. They then use funds from the next person to pay in order to satisfy the account where they stole funds from, and they continue to do this until found out.

- ‘Cheque Skimming’ where an incoming cheque is diverted into a bank account they have opened with a similar name to the companies before it has been recorded obscuring their action by diverting late notices and account statements.
- ‘Refund Skimming’ where weak company controls permit a refund cheque to be diverted by an employee into a bank account the employee has opened with a similar name to the companies before it has been recorded obscuring their action by diverting late notices and account statements.
- An accounts receivable employee credits a customer’s account for a discount, a return, or some other form of write-off. This technique can be used to cover up a previous theft or be used as a form of fraud.
- ‘Fictitious ‘and ‘fictitious accounts’ are typically set up to disguise one another. Company owners might feel compelled to create fictitious sales to make their business seem more profitable to prospective or current clients. Company owners might feel compelled to create fictitious sales to make their business seem more profitable to prospective or current clients. Salespersons who are based on commission might want to create fictitious sales to meet daily, weekly, or monthly goals (especially if there is a tempting target bonus).

DEALING WITH ACCOUNTING FRAUD

4.2 One of the biggest mistakes that any company can make is failing to segregate accounting duties. An employee who is the sole contact for account holders and the books expert has a much easier time getting away with accounts receivable fraud than someone who splits their role with a colleague. Fraud is significantly more difficult to uncover if no one is around to look for it.

4.3 The further steps that companies can take to reduce the risk include:

- Be aware of accounts staff that are either over friendly, or aggressive, assertive, or generally taking steps to make scrutiny uncomfortable or impossible;
- Don’t let one employee have access to every folder, every file, every account.
- Separate accounting functions among multiple employees, if you possible.
- If possible, implement a system where two employees must always be present during key accounting tasks, such as while opening mail or while invoicing customers.
- Be alert to employee problems. some employees who are committing fraud may be openly discussing their financial issues or relationship struggles.
- Implement an anti-theft policy, or a company code of conduct that sets out prohibited behaviour in relation.
- Don’t just implement policies, enforce them. Employees won’t take them seriously if you don’t.
- Make employees aware of the zero-tolerance approach to employee financial misconduct. Explain the consequences of actions.
- Refusing to take holidays, unwillingness to share work tasks, or being unusually close with a customer (or two) are signs that the employee might not want anyone to find their mess.
- Educate personnel (and especially management) about accounts receivable fraud. Suggest comprehensive internal or online training about accounting fraud.
- The more educated and aware that employees are about this form of fraud and it’s warning signs, the more likely they’ll feel comfortable reporting any suspicions.
- Let employees know how they can anonymously report fraud in the workplace. A ‘whistle-blower’ hotline is a good option for this or having an open-door policy.
- Insurance can sometimes cover employee misconduct and minimize out-of-pocket expenses needed to right their wrongs.

Next Week: Part 4 Know Your Supplier