ACTIVE PRACTICE UPDATES

NOVEMBER 2019

dalypark
— Chartered Accountants —
www.dalypark.com
Newry | Lurgan | Belfast

PROTECTING A BUSINESS FROM FRAUD

Steps to shield your firm from threats.

Fraud costs the UK around £190 billion a year, with businesses bearing almost three quarters – £140bn – of those losses.

This worrying picture is backed up by the 2019 Fraudscape report compiled by anti-fraud body Cifas, which provides statistics for fraud committed by employees. The report read:

"Dishonest action by staff to obtain a benefit by theft or deception was the most common type of internal fraud in 2018, accounting for 46%. The most prevalent form of dishonest action during the year was theft of cash from the employer.

"The second most common fraud type was theft of cash from a customer, which rose to 22% in 2018 compared to 17% in 2017."

Fraud can be characterised as rule-bending, but for businesses struggling to manage cashflow it can have catastrophic effects.

Earlier this year, Patisserie Valerie, with a £40 million black hole in its finances, went into administration, saying in a statement that this was "a direct result of significant fraud".

For smaller businesses, of course, it can take much less to cause serious cashflow problems.

WHAT IS FRAUD?

What makes fraud different from mere theft is deception.

A mugger may use violence to rob a victim of cash; a fraudster will achieve the same ends by quietly manipulating the system.

As a result, fraud might take months or even years to detect.

Some common types of fraud carried out by employees include:

Inventory skimming – taking items from stock for resale or personal use. For example, a bartender may take a good bottle of rum, perhaps replacing it with a bottle refilled with a cheaper brand, or chalking it up as wastage.

Expenses fraud – claiming for taxi rides never taken using a handful of blank receipts provided by an obliging driver, or for meals never eaten by altering the date on an old restaurant bill.

Fake invoices – submitting invoices with the name of a supplier, or of a completely fabricated one, but with the fraudster's own bank details, or those of an accomplice.

Procurement – awarding contracts not on the basis of suitability or value for money but to members of their own household, or to business contacts in return for a cut.

Credit cards – buying personal items with the company card, such as fuel, food or, in extreme cases, fur coats.

These schemes rely on the employee having the chance and the employer lacking suitable controls and oversight.

The good news is that with some common sense and good practice, fraud can be tackled.

REDUCING THE RISK OF FRAUD

Before getting into specifics, there are some general principles that can reduce the risk of fraud in your business.

First, there's the concept of 'separation of duties' which states that nobody should be in a position to, for example, raise a purchase order, sign off an invoice and authorise payment.

At some point in that chain, somebody else ought to be involved, sense-checking the payment and scrutinising the details.

There's also a point about culture: it needs to be established that nobody is above being questioned or challenged.

If something doesn't look right, your staff need to feel confident asking the finance director or any other board member to provide the necessary paperwork, which means overcoming the urge to growl at members of your accounts team when they ask awkward questions at awkward moments.

It's also a good idea to think about how you might empower whistleblowers in your firm. The Cifas report recorded an increase in fraud reported by staff, from 11% in 2017 to 17%.

If you give your employees a clear, easy route to blow the whistle on dishonest behaviour by their colleagues, many will.

Another important principle is the importance of documentation.

This has become easier than ever in the age of cloud accounting and digital invoicing, but every expenses claim needs a receipt, every payment needs an invoice and the decision to award any contract should be documented.

Finally, careful and constant monitoring of cashflow, frequent account reconciliation and sound financial reporting will give you the best possible chance of spotting anything amiss.

And here's where the tables turn: owner-operators shouldn't be shy about asking hard questions, or demanding to see evidence, especially where the numbers don't look as they might expect.

INTERNAL CONTROLS

Cifas claimed that the majority (54%) of fraudulent conduct by employees was detected by internal controls and audit.

Thinking about the specific types of fraud listed previously, how might systems and controls help?

In the case of inventory fraud, a regular stocktake by an experienced manager or expert freelancer should probably detect patterns (vodka is always down, but never whisky) or other indicators, such as broken seals on bottles or boxes.

Expenses fraud can be trickier to detect but you can automate certain checks. For example, you might have your accounts system highlight duplicate payments – how likely is it that two taxi journeys in one month would each cost exactly £13.18?

You might also want to flag round payments, which can indicate excessive rounding-up of tips.

At policy level, you can also make it compulsory for expenses to have detailed and specific descriptions – claims for 'miscellaneous' should always be eyed with suspicion.

Fake invoices can be detected through separation of duties, but it's also good to insist that all invoices include a postal address, a phone number, and details of any services supplied.

You might also consider automatically reviewing invoices over a certain threshold value, which is not only a way of detecting fraud but might also act as a deterrent.

Procurement fraud can, again, be tackled through separation of duties. No individual should be able to award a contract without oversight of colleagues.

In general, look out for instances of the same supplier frequently winning work and suppliers who share the same surname or address as the individual managing the tendering process.

Company credit card fraud can be avoided by moving to an expenses system and by scrutinising bills. Payments made over the weekend or during holiday periods are a particular red flag.

Another might be where an employee spends significantly more on fuel for their company vehicle than their peers.

The most important thing is to mitigate the risk of fraud in a systematic way – think about it, talk about it and, if you have one, put it on your risk register.

THREATS FROM OUTSIDE

In 2019, cybercriminals target businesses in various ways.

First, there's a particularly insidious scheme that plays on the anxieties of the operators of small businesses, in the form of emails that claim to be from HMRC, which look official and even appear to come from a government email address.

They may offer unexpected but tempting tax rebates, or suggest that your payment is overdue, or that your details need updating on the Government Gateway.

The aim can vary from stealing bank details to infecting your business's computers with spyware, malware or ransomware.

If you're in any doubt, check the HMRC website for advice before clicking on any links or opening attachments.

Then there are yet more fake invoices, dispatched to lots of businesses in the hope that a handful will be too busy and too careless to check before paying. They typically demand cash for inclusion in a fake or valueless 'business directory'.

Scams like this are best countered through awareness, staff training and IT policy – read up on the latest scams, talk them through with your team and make sure your system has up-to-date malware and virus protection.

Talk to us about managing your business.