8 tips to avoid fraud in your business

WHISTLEBLOWER PARTNERS

Corporate fraud is a major problem that is growing at pace with increased globalisation, digitalisation, and greater complexity in many fields, while coronavirus has exacerbated the issue.

Fraud within companies is a bigger problem than many people think. A company can lose up to 5% of its annual revenue through internal fraud. This has been shown by international studies. Danish companies are also experiencing a sharp increase in financial cybercrime, where employees are tricked into paying money to external criminals.

Control is clearly essential, but while auditing tools, for example, can get you a long way, the solution is not quite so simple. Equally important is a good working culture where employees are encouraged and influenced to make the right choices so that they do not make intentional or unintentional mistakes that can cost the company dearly.

Since the COVID-19 epidemic hit us, homeworking has become the new normal, and this trend is likely to continue. This has also created new risks for businesses.
Here are some points to be aware of in relation to corporate fraud:

1. **Increased control and awareness around procedures in the company**

Fewer people in the office could mean that procedures are relaxed internally to make day-to-day life run smoothly. Passwords may be shared between colleagues, and there is a risk that the same person might approve invoices, change creditor details and approve payments.
This provides obvious opportunities for financial fraud where the fraudster can cover their tracks. If this is done in a small way over a long period, the fraud can become quite extensive before it is – perhaps – detected.
Companies should therefore not relax procedures internally, even if employees are increasingly working individually from home, and should constantly "regulate" control activities in line with risk.

2. **High awareness of hacking, phishing and other IT scams**

Criminals are increasingly trying to trick businesses into giving out personal codes or details via phone calls (vishing), text messages (smishing) or emails (phishing). The fraudster often pretends to be from, for example, the company's bank or a business partner, public authorities, NemID or Nets.
Some companies have their email systems hacked directly, while other fraudsters use phishing, where a click on a link or file in a fake email can give access to the company's IT systems.
It is very important to impress upon employees that they should be sceptical about unsolicited contact or emails that look unusual or strange, and that they should never give out personal details or codes. If in doubt, individual employees should always contact their company's IT department – better one time too many then one time too few.

3. **Avoid CEO fraud**

CEO fraud occurs when an employee is tricked into paying a false invoice or making an unauthorised transfer via the company's account to an account owned by the fraudster. The fraudster pretends to be a senior person in the company in question.

It is important to instil procedures in the company for paying invoices and transferring funds and to ensure that any unusual requests are checked out, no matter how urgently an email may request the transfer. A phone call to the CEO can often expose the whole fraud and save the company from big losses.

4. **Avoid invoice fraud**

In the case of invoice fraud or deception, the fraudster pretends to represent a company's customer or supplier and asks for future invoices to be paid into a new bank account – belonging to the fraudster.

It is important to ensure that the relevant employees are informed about and made aware of this type of fraud and how to avoid it. It is thus essential to instruct staff responsible for paying invoices to always check them for irregularities, to establish fixed procedures for handling manual payments, and to check the legitimacy of payment requests.

It is advantageous to use an automated payment system in order to keep the number of manual payments to a minimum.

5. **Be aware of fraud relating to changes in bank details**

It is important to be aware of the existence of fraud relating to changes in bank details and to ensure that this knowledge is shared with those functions within the company that may be potential victims of such fraud.

If the company receives an email regarding changes in bank details, the supplier should always be contacted to confirm the veracity of the changes with the company's usual contact.

6. **Avoid VAT fraud**

There is a significant risk of businesses being exposed to VAT fraud when trading in relation to VAT carousels. VAT carousels are characterised by the trading of goods or services across national borders. Typically, the goods are traded through a straw man who does not declare or account for VAT when the goods are resold. The goods are then traded through one or more intermediaries before being sent out of Denmark again and continuing the carousel.

These intermediaries may be genuine Danish companies. This means that Danish companies can easily end up in a trap that can lead to financial losses, for example in the form of lost VAT deductions, unsaleable goods, a bad reputation or unfair competition in the industry. In some cases, an entire market can be undermined before the fraud is detected.

If there is the slightest doubt about the supplier or the goods that the company is buying, then you should steer clear of the deal. And it is recommended to always check whether the companies with which the company trades are registered for VAT. The company does this by searching for the supplier's VAT numbers.

SKAT's website also lists a number of specific points to be aware of when buying and selling goods.

7. **Beware of printers**

Printers in businesses can pose a significant security risk for a company if caution is not exercised.

Developments in printer technology, including the fact that printers contain the same hardware components as a computer, such as a drive, control panel and keyboard, mean that businesses should protect printers against attack in the same way as they do for PCs. This is often overlooked even though Danish companies are generally very aware of the cyber threat.

8. **Contact the bank and report fraud or attempted fraud to the police**

If the fraud has been committed through the company's bank, the bank should always be contacted with a view to recovering the amount. Also, always contact the police in case of fraud or attempted fraud, even if you did not actually fall victim to fraud. Remember to keep the documentation and include it in the report to the police.