Protecting your business against External Fraud

Welcome to another edition of our monthly ebriefs, brought to you by Aquila Advisory, the boutique forensic accounting company. In our last issue, Jane Fowler, Managing Director of Aquila, considered ways to protect your business against fraud from within. In this month's issue, we look at the various types of external fraud against a business, how to detect fraud in your business, and how to set up policies and procedures to prevent your business becoming a victim of external fraud.

Firstly, it's important to identify the various fraud risks your business can be exposed to and the ways in which you can protect yourself. Here, we consider three:

- Identity theft
- Cyber attack
- Supplier fraud

Identity Theft

Identity theft is an ever-increasing problem in the UK. According to the Home Office, the annual cost is now £1.7bn, with businesses shouldering around £50m of the burden.

The problem of individual identity fraud is relatively well publicised. Known methods used by criminals to obtain sensitive information include searching through rubbish bins to find discarded bank statements; intercepting mail; copying credit cards during a transaction; and so-called 'phishing' scams, which involve sending emails which look as though they have come from a bank or similar organisation, and asking customers to 'confirm' their details by return email.

But businesses are also at risk and, as well as the potential financial damage, corporate identity fraud could ruin a company's reputation. Businesses are not only subject to all the methods used to steal identities from individuals set out above, but they are also threatened by a growing trend of corporate 'hijacking' – this is achieved when a non-connected entity passes itself off as your company or an individual as one of your directors.

How is this achieved?

Very simply, a fraudster registers themselves as one of your company directors at Companies House and then purchases goods and services from suppliers, which they have no intention of paying for. They will have used your Company House records and registered office address for the suppliers accounts department, and then given a temporary trading address to which the goods should be delivered. Come time for payment, they are long gone leaving you with the bill.

Fraudsters can also make use of publicly available company bank account details and signatures for fraudulent purposes.

Reducing the risk

It's not possible to eliminate risk, but there are steps you can take to protect your business by:

- Securing sensitive documents
- Shredding documents before they are disposed of, particularly blank headed paper and financial correspondence, invoices or statements from suppliers and signed correspondence that you no longer need
- Training staff to raise awareness of identity fraud.

In relation to protecting your business from corporate hijacking, if you have previously filed paper accounts, there is nothing you can do to prevent directors' signatories being on record at Companies House, as the director's signature will be on the Balance Sheet. For all your future filing needs, and for new businesses, file accounts using XBRL, as this files your accounting information electronically so no signatures are included on the accounts. XBRL, or eXtensible Business Reporting Language, is a freely available, open and global technology standard for reporting and analyzing business and financial information.

Your can further protect yourself by signing up for the Companies House Webfiling service and selecting to join PROOF (PROtected Online Filing). The scheme is specifically designed to help companies protect themselves from fraudulent filings as it prevents individuals from filing certain paper forms. The forms covered by the PROOF scheme are:

- Appointments
- Terminations
- Change of Particulars (Company Officers)
- Change of Registered Office Address
- Annual Return

For a belt and braces approach, sign up to the Companies House monitoring service and monitor your own company. Sounds an odd thing to do, I know, monitoring yourself, but it will

alert you to changes made to your company information, however it has been submitted. Any unexpected changes can then be followed up and reported to the police.

Cyber attack

Many attacks may come through your business IT system. Thieves may try to access usernames, passwords and credit card details through 'malware' such as computer viruses, worms, trojans, spyware or adware.

Computer security takes three forms: physically protecting your hardware, electronic protection and educating yourself and your staff on the importance of IT security.

Protect your computers physically

You should:

- Hold regular equipment audits and track movement of computers. Any laptops should be assigned to a particular member of staff whose responsibility it is to keep it safe
- If computers are left in the office unattended, as a minimum secure your premises. And, better still, secure the computer to the desk
- Keep records of serial numbers and identification marks
- Mark your IT with postcodes or passive electronic-marking devices
- Ensure that your staff take care of mobiles and laptop computers when using them away from business premises.

Protect your computers online

You should ensure you have the right IT security installed and that staff understand security processes. Consider the following measures:

- Put an IT security policy in place
- Limit your employees' access to information and restricting access to the level needed for each job, this restricts the information a hacker can obtain through any one log in.
- Keep your passwords and PINs safe and change them regularly
- Use up-to-date anti-virus software
- Install a firewall
- Update all software with patches
- Don't write down your password or other security information, unless it's well disguised.

In relation to access financial data on your computer, protect yourself:

- Always access internet banking by typing the bank's address into your web browser, never search your bank web address. If you are in a hurry you won't spot you are on

HBSC not HSBC … the website itself will look identical, but it will be collecting your data and using it while you are online, gaining access to your accounts

- Never visit a website from an email link to enter personal details - if in doubt, contact the bank separately on an advertised number
- Check your bank's website for safety tips
- Always check your statement thoroughly.
- Look for a locked padlock or unbroken key symbol in the bottom right of your browser window before accessing the bank site - the beginning of the bank's internet address will change from "http" to "https" when a secure connection is made
- Don't leave your computer unattended when logged in to internet banking.

Bank Safe Online www.banksafeonline.org.uk sets out simple steps you can take to keep safe and provides updates on the latest scams. You can also report any suspicious emails or websites via the site.

One final word on the subject of cyber attacks, when disposing of old computers make sure you have wiped them of all information. Or better still, get a professional to do it.

Supplier fraud

Businesses are often the target of unscrupulous suppliers who overcharge, pay staff kick backs for defrauding you, fail to perform contracted work or service, and other actions. Some suppliers/contractors you hire may try to scam you by billing for work they never complete. We know it is important to tender for major contracts and to approve timesheets, check delivery notes etc. However, there is a new scam in town, a variation on an old theme, which is becoming ever more popular….

Here, your business receives a letter purporting to be from one of your suppliers. The letters ask you to amend that supplier's bank account details. It states that all future payments should be settled to a new bank account. You the update your files and subsequent payments are made to this account. But, the reality is that the letter has not come from your supplier at all, but rather from a fraudster.

So, if you receive one of these letters from one of your suppliers, make sure to confirm that the changes are being legitimately requested by checking with your usual contact at the supplier, using existing contact details, not those included in the letter.

If you receive a letter like this, but it is not a supplier you deal with, be kind, do a local search for the company and give them a ring to warn them.

But what do you do if you are the victim of this type of fraud and someone is pretending to be you? It is not you they will be writing to so how will you know it's happening?

Consider introducing these simple controls:

- Educate your customers as to this type of scam and advise them to always check with their usual contact if they receive such a letter purporting to be from you
- Review your debtor accounts regularly for changes in payment patterns. Someone who regularly pays on 30/60 days who suddenly stops paying could indicate they are paying someone else,
- Enforce credit limits on debtor accounts to limit your exposure. Provided you have the right credit limits set this shouldn't hinder business, but will be another alert if the balance owed suddenly increases, indicating a payment has been missed.

In conclusion

The amount of fraud being perpetrated against businesses is getting worse, both in terms of the number of instances and the amount of money that is being lost, and some of this can be attributed to the difficult economy.

For small and mid-sized businesses, the vulnerability to fraud can be compounded because of the sometimes informal nature and the fact that there are fewer staff members, therefore fewer checks and balances.

Given that fraud against your business can impact the bottom line, it's important to set up procedures now, to verify adherence to anti-fraud policies and to detect and deter possible business fraud. And, if you suspect or discover fraud you should act immediately to limit the damage caused to your business' bottom line and reputation.

At Aquila Advisory, we work with businesses across all sectors, helping them and their clients to implement anti-fraud policies. We understand the impact a fraud can have on a business and, where a fraud is suspected, we undertake discreet work to investigate suspicious activity, detect fraud, collate evidence and advise on the appropriate course of action.

So contact Aquila today for a free initial consultation and to find out how we can help you protect your business against fraud.

CONTACT AQUILA ADVISORY:

Jane Fowler, Managing Director

Tel: 020 7397 8318
Email: info@aquilaadvisory.co.uk
Website: www.aquilaadvisory.co.uk