




Commercial Information Solutions

Your Guide to Combating Corporate ID Theft & Fraud

INFORM › ENRICH › EMPOWER



A blue-tinted photograph of a person's silhouette looking out a window with a grid pattern. The person is in the center, looking towards the left. The window has a grid of dark lines. The background is a bright, hazy blue sky. The overall mood is contemplative and somewhat somber.

**The result:
lost profits,
lost reputation
and even, in
some cases,
liquidation.**

Too busy to spot fraud?

The dedicated Commercial Fraud team at Equifax has seen an increasing prevalence of frauds being committed against small and medium sized businesses.

Could this be one of the consequences of the recession? Business managers and owners, already under increased financial pressure, have limited time to ensure they aren't falling foul of clever fraudsters. Unfortunately, the fraudsters know this and are making the most of the opportunity. Here we examine the issues of corporate identity fraud and the challenges facing UK companies in tackling this risk.

Imagine this picture

A successful business suddenly discovers that it has huge debts against its name – debts it knew nothing about. Creditors are now after the company directors for payment. The company's success is rapidly undermined – not just by financial losses, but by the loss of reputation that ensues. The result: lost profits, lost reputation and even, in some cases, liquidation.

Sounds unlikely? Unfortunately it is the reality for many UK companies, as corporate ID theft and fraud become ever more common.

It has been estimated that corporate ID theft and fraud is costing UK business millions of pounds a year, with many organisations suffering serious consequences to cashflow and even ongoing success as a result. The issue of corporate ID theft and fraud must, therefore, go higher up the agenda for companies and organisations, as quickly as possible.

The more successful
you are, the more
likely your company
will become a target
for fraud.

› Commercial Information Solutions

'That will never happen to me!'

That must be the thought of many CEOs, MDs and FDs when they hear about another company becoming a victim. Corporate fraud is often seen as something that happens to the company next door. But the reality is that the risk is much closer to home. The more successful and established the company, the more likely it will be a target for fraud. After all, there is no point targeting an unsuccessful business.

Safety in numbers

Indeed, large corporates that think they have all the precautions in place through their risk management policies should not be lulled into a false sense of security. There are as many reports of large businesses being victims of corporate ID theft and fraud as smaller companies.

All companies and businesses are at risk of becoming a victim of fraud and deception.

The argument could even go that large corporates are more vulnerable because of the complexity of systems and the ease with which activities could be 'hidden'.

But, the reality is all companies and businesses are at risk of becoming a victim of fraud and deception, and need to implement what are often simple precautions to provide the necessary protection from what could be a very expensive threat.

Know the risks

There are a variety of systems available to help you protect your company from corporate fraud, but being aware of the problem is the first step to closing the net on the criminals.

There are a number of commonly used types of corporate fraud. In each case, you can take what are often simple precautions to keep fraudsters at bay. And, by knowing the risks you can go a long way to minimising them.

Call us on **0800 032 4980**

Company identity fraud

Company identity fraud, also known as company hi-jacking, is similar to personal identity theft. The truth is it's easy to change company documentation and Companies House has to accept documentation it receives at face value. Without a great deal of knowledge or effort, a fraudster can change your registered office, trading address, even the names of your company directors – all without you knowing.

The fraudulent details would appear official in any checks undertaken on your company. In addition, an ordinary credit search against the business, with any of the credit reference agencies, is likely to show a healthy credit rating. So there's no reason for a supplier not to accept an order.

This is when the fraudster's fun begins. Having changed your address, and using your name, they can order goods from current or new suppliers and have them delivered to the new address. Suppliers carrying out a check on the details kept at Companies House will be unaware of any criminal activity and, using your own well-established credit rating, will dispatch goods to the fake address.

Of course, you will not see these goods, the supplier will not be paid and you will both be blissfully unaware of the situation – until the supplier chases you for payment. By then, the

fraudster is long gone with the goods, leaving you to deal with the consequences.

At least two victims

There will always be at least two direct victims of company identity fraud: the company whose details are taken and the company that supplies the goods or services. Ultimately, everyone pays through higher product costs and insurance premiums.

The steps to help prevent company identity fraud are relatively simple, and while not 100% foolproof, go a long way to protecting your business:

- never throw out company documentation showing letterheads, signatures, bank account and company credit card details or invoices – make sure all business documents are shredded or disposed of securely
- file your documents at Companies House electronically using their Proof system – this will undoubtedly help the situation, but will not stop it completely
- invest in a monitoring service that will alert you to any changes in your company details held by Companies House, such as Equifax Portfolio Monitoring. This allows you to take immediate action if changes are made and ensures you do not become an unwitting accomplice in this kind of fraud.



**If they have
nothing to hide,
a personal credit
check shouldn't
cause a problem.**

› The Heart of Data Intelligence

Long firm fraud

Long firm fraud is where an apparently legitimate business is set up with the purpose to defraud by obtaining goods, with the intention of evading payment for them. The business sets about developing a decent credit history to win your trust, which they do by placing numerous small orders and ensuring they pay promptly.

When the fraudsters are ready they will place several larger orders with most or even all of their suppliers at the same time. On receipt of the goods the criminals promptly disappear and sell them on from various trading places.

Most long firm frauds are set up with the purpose to defraud at a point in the future. This means they can disappear before they have to file any accounts at Companies House.

Stop and think

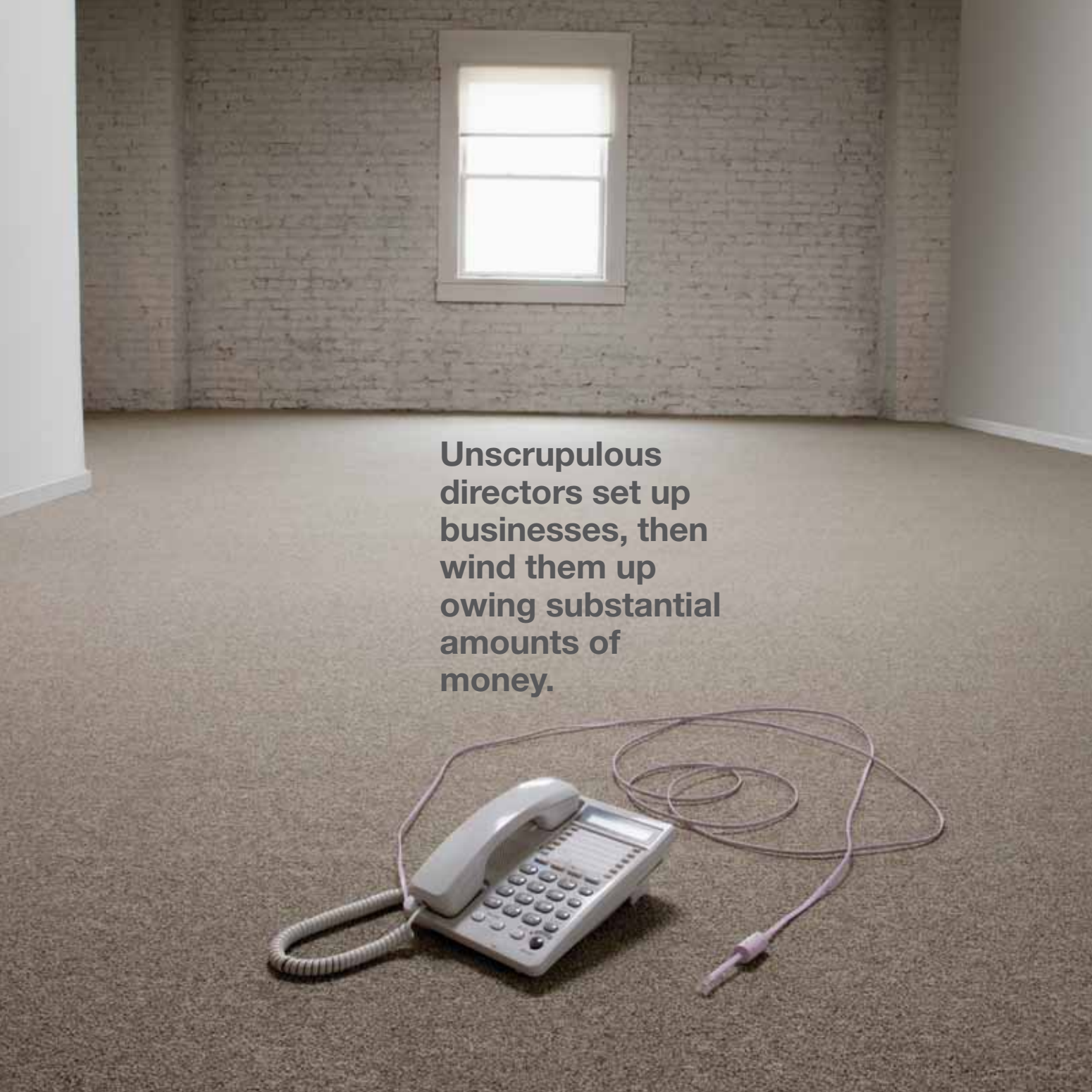
Before accepting a much larger order from a company that you have been dealing with for a relatively short period, stop and think about whether you have asked enough questions and know enough about them, even if they have been prompt payers in the past.

You should also check the trading history of the businesses you are dealing with. The key thing to look out for is any connection to dissolved

companies in the past. Even if the previous dissolved company looks like it could have been voluntarily wound up, beware! This does not mean that no one had their fingers burnt.

Also get consent to check the credit histories of the individuals in the business. If they have nothing to hide then this should not cause a problem. Most people now accept that, if a business is relatively new, suppliers will want to check the personal details of the company's directors or owners before advancing credit.

You could also check for evidence that they reside where they say they do and find out if there is any data held on them that could be of concern. County Court Judgments and bankruptcy information, for example, provide vital clues to an individual's trading history.

A photograph of an empty room with a brick wall, a window, and a telephone on the floor. The room is mostly empty, with a brown carpeted floor and a white baseboard. A window with a white frame is centered on the brick wall, letting in bright light. A white telephone with a coiled cord and a long, thin cord is lying on the carpet in the foreground. The text is overlaid on the right side of the image.

**Unscrupulous
directors set up
businesses, then
wind them up
owing substantial
amounts of
money.**

› Commercial Information Solutions

Phoenix companies

Another type of corporate fraud is phoenix company fraud. This is normally when a director or directors set up businesses, then wind them up owing substantial amounts of money. The directors then create another company operating in the same field, often using a similar or even the same company name. Creditors of the original company lose out when the company goes bust. The directors have no financial responsibility to settle the debts – yet they can start up again with no negative impact.

Can you trust the references?

To help your company avoid getting caught out by phoenix company fraud make sure you investigate any trade references given and try to ensure that these are truly independent references.

As with long firm fraud, checks should be carried out on the directors themselves. Check their history with other companies and, with consent, check out their personal credit history.

When checking previous directorships, note if previous companies have similar or same names to the one you are now dealing with. If so, ask why that company was dissolved. Remember, even if it looks like a voluntary dissolution that does not mean no one has lost out.

Often, perpetrators of phoenix company fraud leave behind lots of relatively small debts, probably resulting in no individual creditor seeing it as financially viable to take the matter further.

The directors
have no financial
responsibility to settle
the debts – yet they
can start up again
with no negative
impact.

Call us on **0800 032 4980**

› The Heart of Data Intelligence

Criminal takeover

Another form of company hi-jacking is when long established and well-run companies are targeted by fraudsters – often organised crime syndicates – who literally ‘hi-jack’ the company by investing in the business and appointing a member of the syndicate to the company’s board of directors.

Often, the original directors resign and are replaced by other syndicate members until the original company is totally in the hands of organised crime.

Know who you’re doing business with

When you have a new order, don’t simply rely on previous credit checks – look at information other than the accounts.

Check for board-level changes; if there have been a number of changes over recent months ask yourself if this customer still represents the entity that you had dealt with in the past. If there have been significant changes you may be dealing with a totally different entity than the one that has built up a great trading history with you previously.

With the right service from your credit reference agency the cost of reviewing a company’s details is negligible.

Newly incorporated companies

Probably the most worrying fraud is where newly incorporated companies file accounts at Companies House, but the facts are literally too good to be true in terms of the turnover and profits earned by a new start-up in their first year of trading.

The aim is to use the good credit rating thus obtained to buy goods on credit and disappear without paying. Businesses who are currently eager to secure new clients and business will be particularly vulnerable to this form of fraud.

The facts are literally too good to be true in terms of the turnover and profits earned.

Find out about the directors

As with long firm fraud and phoenix companies, checks should be carried out on the directors themselves. Check their history with other companies and, with consent, check out their personal credit history.

Keeping your business under lock and key

Protecting your business from the diversity of corporate frauds that now prevail is just like looking after your home. You wouldn't go out leaving doors and windows unlocked or let a stranger into your home.

By taking simple precautions, you can better protect your company from the risks. What's more, the costs don't need to be too great, especially when compared with the losses if your business is hit.

A company that has been victim to some form of corporate fraud or theft often sees its losses in terms of immediate financial costs. But, a longer-term loss could be in the form of lost reputation. Customers might not want to deal with them in the future because their confidence in the company's security and stability has been knocked.

There is also the issue of insurance costs. While your insurance might provide some cover, you will never receive complete recompense. And as soon as a claim is made your premium goes up.

Individual losses as a result of corporate fraud or theft can go into the tens of thousands of pounds. But the cost of protection can be minimal.

Don't just monitor customers

Unfortunately, many directors fail to appreciate the value of monitoring their own company and credit information. Feedback from some Equifax customers suggested that they avoided monitoring services simply because they didn't want to be bombarded with alerts, and concerns over the costs of each alert.

Addressing both of these issues, Equifax Portfolio enables you to build multiple profiles that are simple to use and easy to maintain. Setting up a unique profile of your own company or group of companies is quick and easy.

And, because you have the ability to set the criteria most important to you, the alerts you receive provide a direct link to the information you chose as critical to making profitable credit decisions.

Prevention is better than cure

Whatever services you decide to use, prevention is better than cure. Simple checking processes should be mandatory when dealing with new or existing customers and suppliers and, for the most effective protection, everyone in your company should be trained on those processes.

Remember, relatively low-cost monitoring services can provide the important back-up you need to catch clever fraudsters.

12 ways you can reduce the risk of corporate ID theft & fraud affecting your company

Protecting your company from the devastating effects of corporate ID theft and fraud does not have to be costly or complicated.

The following tips, actions and procedures are highly effective, yet simple to apply

1. Identify business partners and directors – check personal credit references as well as for the business.
2. Confirm fax and telephone numbers, email and website addresses, and never accept hand written order forms or faxes.
3. Confirm the trading address of customers.
4. Ask for original headed company paper.
5. Are you sure they are who they say they are?
6. Did they answer your call with a business name?
7. Don't assume information provided is correct, always double-check and follow up the references.
8. Are all references truly independent?
9. Can they provide trade or bank references?
10. Check that the telephone area code is relevant to where the business claims to be trading from.
11. Check for any connections to previous companies with similar or identical names.
12. Monitor your own company details at Companies House.

Online support

Cost effective and easy-to-use online tools can help provide the answers you need to protect your company from ID theft and fraud.

Automated alerts, for example, offer a quick and reliable way to monitor for important changes, while access to a comprehensive range of intuitive online reports provides the flexibility you need to assess risk levels before distributing goods or extending credit terms.

If you have already become a victim

Corporate fraud and theft can have a serious impact on a business. So it's important to rectify this as quickly as possible.

Five steps you should take

1. Report the matter to the police and other relevant organisations such as Companies House, suppliers, etc.
2. Reassess your organisation's risk management and control systems to make sure you aren't likely to fall victim again.
3. Keep a record of all correspondence you make or receive in respect of the fraud.
4. Inform your customers if their details may have been compromised too or a fraudster may have contacted them, purporting to be from your business.
5. Obtain an up-to-date copy of your organisation's credit report and check your Companies House record for any discrepancies. Both Equifax and Companies House provide a way for you to get corrections made to your records.

Corporate fraud can have a negative affect on the value of your brand as well as the stability of your bottom line.



› The Heart of Data Intelligence

Spotting the fraudsters

Equifax analyses Companies House records, directories information and a wealth of other data sources. Furthermore, the Equifax Commercial Fraud team regularly interrogates our own commercial databases for unusual access patterns on particular business's credit reports. These might be out of keeping with previous access patterns or are from companies that operate in completely different business sectors and can be an excellent indication of a long firm fraud being perpetrated.

The Equifax team also closely examine the accounts of new start-up companies with no previous trading history behind them. Here they are checking that the accounts have a basis in reality and are not simply filed at Companies House for the purpose of obtaining a favourable credit rating with which to defraud legitimate businesses. And they work closely with Operation Sterling, an economic crime strategy team set up by The Metropolitan Police Service which is working in partnership with Companies House to combat fraud targeted at UK businesses.

Tools to protect your business

Identify potential risk, with Optima

Providing many of the features you need to help prevent corporate ID theft and fraud, Optima allows you to review a company's details, cross reference directors, and reveal a company's entire group structure.

Predict fraudulent activity, with Protect

Protect is a unique alert code scoring system that analyses the past performance of directors and evaluates the risk of fraudulent activity or losses from dealing with companies that have been badly run.

Expose risky directors, with Connections

Connections helps you to identify directors that may have tried to hide past performance by breaking links to previous companies.

Automate alerts with Portfolio Monitoring

Portfolio Monitoring allows you to monitor your business, and the companies you trade with, for key changes that could indicate potential fraud.

Put Equifax at the heart of your fraud prevention strategy

Call us on 0800 032 4980 or email commercial.risk@equifax.com

EQUIFAX[®]

COM1217SC/October 2009

Equifax Plc
Registered office: Capital House,
25 Chapel Street, London NW1 5DS

Registered in England No: 2425920

Equifax is a registered trademark of Equifax Inc.
Copyright © 2009, Equifax Inc. Atlanta, Georgia.
All rights reserved.

www.equifax.co.uk

INFORM ➤ ENRICH ➤ EMPOWER