FRAUD FACTS

Fraud Advisory Panel

Issue 1 September 2011 (2nd edition)

INFORMATION FOR ORGANISATIONS

# Corporate identity fraud

**The term 'corporate identity fraud' is commonly used to describe the impersonation of another company for financial or commercial gain. Fraudsters steal your company's identity and/or financial information and use it to purchase goods and services, obtain information or access facilities in your company's name.**

## What is corporate identity fraud?

Corporate identity fraud is the criminal use of a company's identity to obtain goods, money or services by deception.

It occurs when a fraudster steals your company's identity and/or financial information and uses it to purchase goods and services, obtain information or access facilities in your company's name.

Companies House estimates that about 10 cases of corporate identity fraud occur each month. Individual cases often have significant value and can cause serious disruption to a company's business and damage its reputation.

## Common types of corporate identity fraud

**Company hijacking:** A fraudster submits false documents to Companies House to change the registered address of your company and/or appoint 'rogue' directors. Goods and services are then purchased on credit, sometimes through a reactivated dormant supplier account, but they are never paid for.

**Company impersonation:** A fraudster impersonates your company (sometimes by purporting to be a director or key employee) to trick customers and suppliers into providing personal or sensitive information which is then used to defraud them. Your company may be impersonated using phishing emails, bogus websites and/or false invoices.

## How does the fraud work?

A fraudster acquires or steals information about your company. This may include:

- your company's name, registered office address, and company and/or VAT registration number;
- information relating to your directors and/or employees obtained from social networking websites (eg Facebook, MySpace and LinkedIn) and other sources such as local council records;
- email domain names and telephone numbers (including mobile and 0845 numbers) obtained from your company website;
- bank account details;
- supplier and/or customer account information.

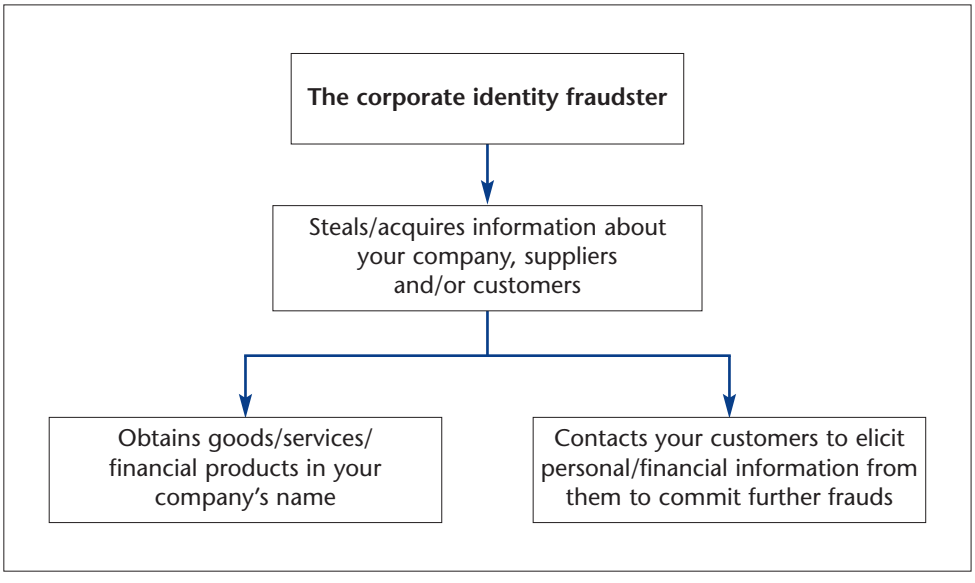
This information is then used to:

- acquire financial products (eg loans and corporate credit cards)
- order goods and services on credit
- hijack company bank accounts
- make VAT claims
- deceive customers
- purchase assets

all in your company's name.

Sometimes a fraudster will change your company's details (eg directors or registered office address) with Companies House in order to facilitate criminal activity such as money laundering or to fund drug trafficking and/or terrorism.

Companies can be vulnerable to corporate identity fraud committed internally by employees (who have been compromised either by their own financial circumstances or by a third party such as a criminal gang), externally by individuals or organised criminals, or in collusion.




## What happens if your business becomes a victim?

Corporate identity fraud can have a financial and reputational impact on your company. You will need to limit the damage caused by the fraudster (particularly to your credit rating) and this can take time.

Five steps that you should take:

1. Immediately report the matter to the police and other relevant organisation(s). Also consider reporting it to Action Fraud by calling 0300 123 2040 or visiting the website www.actionfraud.org.uk. Follow their advice.
2. Inform your customers if their details may have been compromised or they may have been contacted by a fraudster posing as a 'representative' of your business.

3. Obtain copies of your business's credit report (available from credit reference agencies) and Companies House record. Check for discrepancies. Go back to step 1 if necessary.
4. Keep a record of all correspondence you send or receive in respect of the corporate identity fraud, including any communications you may have with the fraudsters themselves.
5. Reassess your company's risk management and control systems to ensure that your business is adequately protected. Change relevant passwords and PINs.

You may also wish to consider hiring a professional to prepare witness statements on your behalf, to act as a liaison with the police, and to identify other potential victims.

## Legal recourse

**Criminal prosecution:** Corporate identity fraud is a criminal offence and the police will consider taking criminal action if you refer the matter to them promptly.

**Civil recovery:** Civil recovery may enable your company to recover some of its stolen assets. Legal advice should be sought.

## How to protect your company

Be aware of the risk from corporate identity fraud and safeguard your company's information.

**DO:**

- ✔ Develop and implement a zero-tolerance culture incorporating an anti-fraud policy and fraud response plan. Clearly communicate it to all employees. Review it on a regular, preferably annual, basis.
- ✔ Conduct pre-employment screening on all new employees before they start work. Consider periodic checks on existing employees in high-risk areas or on promotion.
- ✔ Securely destroy all confidential and sensitive business information. Shred paper, CDs and DVDs. Wipe computer and mobile device memories before disposal.
- ✔ Store confidential or sensitive information in a secure place. Limit access to essential staff.
- ✔ Check your company's registered details at Companies House on a regular basis. Register for WebFiling, PROOF and Monitor services.
- ✔ Review your credit report for discrepancies on a regular basis.
- ✔ Educate staff about fraud prevention and detection as part of your induction programme and on an ongoing basis.
- ✔ Conduct checks on new and existing business partners, customers, suppliers and third-party service providers. Be alert to changes of ownership or unusual trading patterns of those you deal with.
- ✔ Arrange for your mail to be redirected (for at least a year) if you move business premises and notify vendors, customers and other partners of your change of address.
- ✔ If you don't receive any mail, check with Royal Mail to ensure that a redirection hasn't been set up in your company's name without your knowledge.
- ✔ Implement a clear desk policy for all staff.
- ✔ Establish a credible mechanism for staff to report suspicions of fraud.
- ✔ Encourage a 'no blame' culture where issues can be discussed without recrimination.
- ✔ Ensure your IT security policy covers mobile devices, laptop computers, the internet, email and access. Review it on a regular basis.
- ✔ Keep computer security software (such as anti-virus and anti-spyware) and firewalls up to date.

**DO NOT:**

- ✗ Assume that the information provided by prospective employees is accurate. Independently verify it.
- ✗ Give employees unlimited access to confidential and sensitive information unless it is necessary.
- ✗ Rely solely on information obtained from Companies House when checking a new supplier's or customer's credit history. Use other credible sources.
- ✗ Put business bank account details and directors' signatures into the public domain (eg on your website). It is important to note that signatures will be available on the public record if you file paper documents with Companies House rather than filing electronically.
- ✗ Allow employees to keep a written record of business passwords.

## Further information

**Action Fraud**
www.actionfraud.org.uk

**CIFAS – the UK's Fraud Prevention Service**
www.cifas.org.uk

**Companies House**
www.companieshouse.gov.uk

**Fraud Advisory Panel**
www.fraudadvisorypanel.org

**HM Revenue and Customs**
www.hmrc.gov.uk

**Identitytheft.org.uk**
www.identitytheft.org.uk

**The Insolvency Service (Companies Investigation Branch)**
www.bis.gov.uk/insolvency/Companies/company-investigation

*The Fraud Advisory Panel gratefully acknowledges the contribution of CIFAS – the UK's Fraud Prevention Service, Tim Harvey (Association of Certified Fraud Examiners) and Mia Campbell (Fraud Advisory Panel) in the revision of this Fraud Facts.*

Fraud Advisory Panel, Chartered Accountants' Hall, Moorgate Place, London EC2R 6EA.
Tel: 020 7920 8721, Fax: 020 7920 8545, Email: info@fraudadvisorypanel.org.
Company Limited by Guarantee Registered in England and Wales No. 04327390
Registered Charity No. 1108863

**Distributed by**

### Disclaimer

Dissemination of the contents of this Fraud Fact Sheet is encouraged. Please give full acknowledgement of the source when reproducing extracts in other works. While every effort has been made in the preparation of this Fraud Fact Sheet, compliance with it does not guarantee that you will not be a victim of fraud or criminality aimed against you. The Fraud Advisory Panel and the contributors of this Fraud Fact Sheet accept no responsibility for any action taken by parties as a result of any view expressed herein. Readers are strongly advised to seek and obtain the appropriate professional advice on the issues raised which affect them.

© Fraud Advisory Panel 2011