FRAUD FACTS

Fraud Advisory Panel

Issue 1 October 2008

INFORMATION FOR ORGANISATIONS

Corporate Identity Fraud

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

What is corporate identity fraud?

According to the Home Office Identity Fraud Steering Committee corporate identity fraud occurs 'when a false corporate identity or another company's identity details are used to support unlawful activity'.

Common types of identity fraud

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

Company impersonation: A fraudster impersonates your business to trick customers and suppliers into providing personal or sensitive information which is then used to defraud them. Your business may be impersonated using phishing emails, bogus websites and/or false invoices.

How does the fraud work?

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

- Your organisation's name and company number (if incorporated)
- The address of your registered office
- Information relating to your directors, employees or customers
- Details of your supplier accounts

This information is then used to:

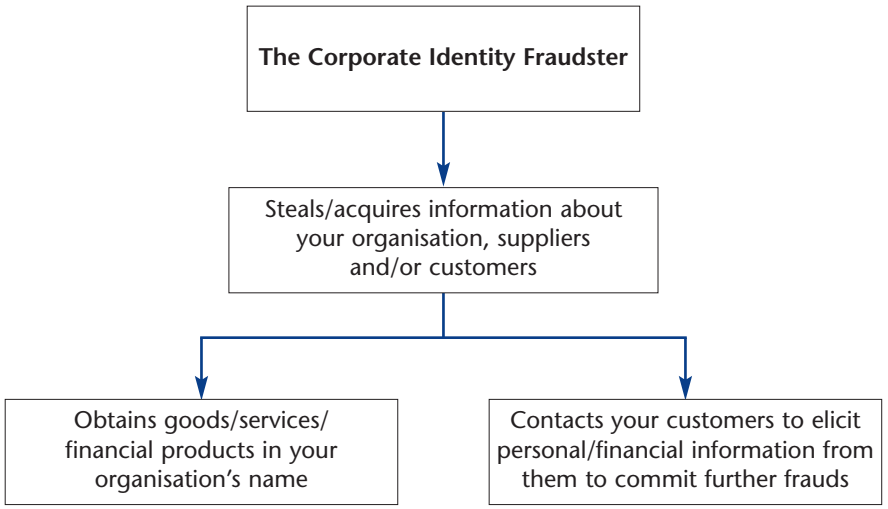
- Acquire financial products (eg, loans and corporate credit cards)
- Order goods and services on credit
- Hijack company bank accounts
- Deceive customers
- Purchase assets

All in your organisation's name.

Sometimes a fraudster will change your business's details (eg, directors or registered address) with Companies House in order to facilitate the criminal activity.

Alternatively a fraudster may simply set up a false company to purchase goods and services on credit from your organisation and disappear before paying for them.

Organisations can be vulnerable to corporate identity fraud committed internally by employees, 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 organisation. You will need to rectify the damage caused by the fraudster (particularly to your credit rating) and this can take time.

5 steps that you should take:

1. Report the matter to the police and other relevant organisation(s) immediately (eg, suppliers, Companies House). Follow their advice.

2. Inform your customers if their details may have been compromised or a fraudster may have contacted them as a 'representative' of your business.
3. Obtain copies of your organisation's credit report (available from credit reference agencies) and Companies House record and check for discrepancies. Go back to step 1.
4. Keep a record of all correspondence you make or receive in respect of the corporate identity fraud.
5. Reassess your organisation's risk management and control systems to ensure that your business is adequately protected.

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: An alternative to criminal prosecution which may enable your business to recover some of its stolen assets. Your business should seek legal advice.

Further information

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

Companies House
www.companieshouse.gov.uk

Fraud Advisory Panel
www.fraudadvisorypanel.org

Home Office Identity Fraud Steering Committee
www.identitytheft.org.uk

How to protect your organisation

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

DO:

- ✔ Develop an anti-fraud policy statement and clearly communicate it to all employees.
- ✔ Ensure that checks are carried out on all new employees including references, qualifications, experience and past employment.
- ✔ Securely destroy all documents containing confidential or sensitive business information before disposing of them.
- ✔ Store confidential or sensitive information in a secure place and limit access to key employees.
- ✔ Check your business's registered details at Companies House on a regular basis.
- ✔ Register for Companies House PROOF scheme and monitor service.
- ✔ Review your credit report on a regular basis.
- ✔ Include fraud prevention and detection within your induction programme for all new employees and provide ongoing fraud awareness training to all employees.
- ✔ Undertake checks on all new customers and review existing customers on a regular basis.
- ✔ Implement a clear desk policy.
- ✔ Encourage a 'no blame' culture where issues can be discussed without recrimination.
- ✔ Introduce a whistleblowing policy and clearly communicate it to all employees.
- ✔ Ensure your IT security policy covers mobile devices, laptop computers, the internet, email and access. Review it on a regular basis.

DO NOT:

- ✗ Assume that the information provided by prospective employees is accurate. Independently verify it.
- ✗ Give employees unlimited access to sensitive or confidential information unless it is necessary.
- ✗ Rely solely on information obtained from Companies House when checking a new customer's credit history. Use other credible sources.
- ✗ Put business bank account details and directors' signatures into the public domain (eg, on your website).

The Fraud Advisory Panel gratefully acknowledges the contribution of CIFAS – the UK's Fraud Prevention Service, Samantha Whitlock (ASB Law) and Mia Campbell (Fraud Advisory Panel) in the preparation of this Fraud Fact Sheet.

Fraud Advisory Panel, Chartered Accountants' Hall, PO Box 433, Moorgate Place, London, EC2P 2BJ.
Tel: 020 7920 8721, Fax: 020 7920 8545, Email: info@fraudadvisorypanel.org.
Registered Charity No. 1108863

Distributed by