

Identity fraud – a growing menace

THE COST TO THE UK ECONOMY OF IDENTITY FRAUD IS estimated at £3.5bn per annum. While most publicity is about the individuals who have fallen victim, corporations have also suffered substantial losses through the impact of ID fraud. This loss can result both from the damage caused to a business when its identity is stolen and the damage that can be caused when third-party information held by a business falls into the hands of an unscrupulous third party.

Fraud levels are at their highest in ten years. In 2005, 222 fraud cases came before the courts, with a total value of £942m, up from £329m in 2004.

The government was the hardest hit, to the tune of £448m, while the private sector suffered a loss of £360m.

The main perpetrators were not one-off criminals but were divided between employees and professional criminals, each accounting for £421m. (Source: KPMG fraud report, 30 January 2006.)

VULNERABILITIES TO BUSINESS

Employee fraud

The threat from within is one of the biggest problems facing UK businesses. Recent figures show that employee fraud rose by more than 80% in 2005.

Unscrupulous employees with access to confidential customer information may use it to create false identities, which are in turn used for personal gain by fraudulent means. Alternatively, they may use information about the company to defraud others, who believe they are dealing with the company itself.

In the UK, 29% of directors and 17% of middle-managers leave their companies with confidential information. Employees are becoming increasingly sophisticated in their approach to removing customers' details from IT systems and avoiding detection. An example is the case of a help-desk employee, working for a company with access to customer credit reports. He, along with others,

spent more than two years pilfering information from the credit reports and using it to siphon funds from customer bank accounts and make fraudulent purchases.

It is often the case that low-level employees are given access to details of customers and suppliers and that the screening of these employees is frequently inadequate. The chairman of the Financial Services Authority (FSA) has said: 'There is increasing evidence that organised criminal groups are placing their own people in financial services firms so that they can increase their knowledge of the firms' systems and controls and thus learn to circumvent them to commit their frauds.'

There can be additional risks with system access being given to temporary employees and consultants. Businesses will set up temporary computer accounts for such staff, but these accounts are frequently left operational long after the temporary staff have left the company. The potential is there for that member of staff to continue to gain access to the company's system and remove confidential information.

Employees can also be the target of criminal gangs, who have been known to drink in the same bars. In a relaxed social environment, disgruntled and vulnerable employees are identified and can be cajoled, bribed or threatened into supplying confidential information.

Employees can also unwittingly provide information to criminals. Confidential information that has been removed from the workplace for wholly innocent reasons may be stolen. A laptop stolen from the car of an Ernst & Young employee contained the financial details of 243,000 customers of Hotel.com. Company laptops are frequently stolen and yet businesses still only require them to have the most rudimentary security systems installed.

Employees working on their home computers are also likely to have less sophisticated security systems than on their work computers. This may allow hackers to access confidential information about customers and business partners kept on these computers.

When vulnerabilities in a company's system are exploited to enable third-party data to be used to commit ID fraud, not only can this damage confidence in the company, but it may also result in the company being liable for losses suffered – eg under the Data Protection Act, if it has failed to take sufficient steps to keep data secure.

'Unscrupulous employees with access to confidential customer information may use it to create false identities.'

Anthony Riem, partner, PCB Litigation LLP
E-mail: ajr@pcbllitigation.com



Corporate identity theft

Businesses can have their identities stolen as well as people and there does not necessarily have to be a weakness in their systems for this to happen. It is the trust of customers and suppliers in the business with which they believe they are dealing that makes these scams so effective.

The internet is a fraudster's charter. It provides an anonymous and cheap method of access to customers and businesses. Unsuspecting customers and suppliers who are not internet-savvy may easily fall foul of imitation company websites.

- **Phishing**

Phishing (an amalgamation of the words 'password harvesting' and 'fishing') is a crude but effective method of acquiring confidential information from the unsuspecting customer. E-mails, purporting to be from a bank or major online merchant, are sent to customers, who are asked to click on a link and verify their account details. The link actually takes them to a fake website, often indistinguishable from the genuine business website, and the customer provides their log-in details, passwords and even financial details.

- **Vishing**

Vishing, a variant on phishing, relies on voice-over-internet-protocol (VoIP) services. Victims receive an e-mail or automated telephone call purporting to be from their bank or other major merchant. They are asked to call a specified local telephone number that appears to be a company telephone number. A further automated voice requests their 16-digit card number for account verification purposes.

The genuine business may suffer immeasurable damage to its reputation – and the greater the reputation, the greater chance of the scam working. It is important that customers are made aware of the risks and that they understand how to verify approaches made to them requesting confidential information.

- **Website hijacking**

This is another internet-based corporate ID theft that can hurt businesses. The most common form of website hijacking is spambots. These collect e-mail addresses from websites with the intent to spam the owners of the website. If there is an e-mail address located anywhere within the company website, a spambot can find it. The loss to businesses that become victims of this type of ID theft is the time spent dealing with spam e-mails. There is also the potential for

virus infection of the system on opening a seemingly innocent e-mail that turns out to be from a hijacker.

Websites may also be hijacked by a competitor that redirects customers to its own website. Companies have been known to use spyware, which watches what a user is doing on a rival company website and redirects the customer as they finalise their order. The aim is clearly to steal customers and the hijacked company can lose financially and suffer from damage to its reputation. It is often only when the company is informed by a loyal customer or business suddenly drops for no apparent reason that the victim company becomes aware of the problem.

- **Companies House**

Companies House has come under fire for weaknesses in its system that have allowed criminals to defraud businesses. PCB was last year instructed on a case of alleged corporate identity theft involving Companies House. The allegation was that various forms had been filed with Companies House purporting to change the shareholders, director and secretary of the company PCB represented, without proper authorisation. It was claimed that the company in question held assets worth in excess of \$35m.

The case highlighted how easy it is to effect changes at Companies House in a way that could be used to deceive third parties as to the identity of the person with whom they are dealing.

In that case, while the claimant obtained various interim injunctive relief in relation to the company, PCB succeeded in having the claim struck out before freezing the claimant's assets in five different jurisdictions to secure the costs, on the basis that the claimant was himself a fraudster!

Fraudsters have also changed the registered office and trading address details for a particular company via the Companies House filing system. Companies House call this hijacking. Orders are placed with suppliers, but delivered to fake addresses without the knowledge of the company. In these cases, the goods are not paid for and eventually the victim company is invoiced. (Source: www.equifax.co.uk, 26 July 2006.)

Companies House admits that it cannot prevent hijacking. It does not have the power to investigate the contents and accuracy of forms >

'Companies have been known to use spyware, which watches what a user is doing on a rival company website and redirects the customer as they finalise their order.'

sent in for filing. A system has been developed that allows companies to register for authorisation codes, without which certain forms will not be accepted. The system also allows for certain forms to be accepted only when filed online. However, breach of this system simply requires the fraudster to acquire the authorisation codes.

There are normally two types of victim in this fraud, the business supplying the goods or services and the customer. The results are higher insurance premiums and damage to the reputation of possibly both businesses.

CONCLUSION

All parties need to have confidence and trust in the systems they use. Businesses must demonstrate that controls are properly designed and operate effectively to reduce the risks of ID fraud. As businesses accumulate and store increasing volumes of confidential information, the responsibility to manage the security of this information likewise increases.

*By Anthony Riem, partner, international fraud and commercial litigation, PCB Litigation LLP.
Tel: +44 (0)20 7831 2691.
www.pcblitigation.com.*