

Knowledge is power: limiting liability and losses



BY ANTHONY
RIEM
partner, PCB
Litigation LLP



BY LUCY
HAMILTON-
JAMES
solicitor, PCB
Litigation LLP

IN SOME OF THIS SERIES OF ARTICLES ON CYBER crime we have looked at the ways in which cyber crime, and in particular, identity theft, is committed. We have also explored some of the ways in which the unsuspecting victim may become liable themselves and the pitfalls of self-help investigations by victims.

This article is intended to consolidate the main points previously detailed in those articles and identify some of the ways in which victims and potential victims of cyber crime can limit or prevent loss and liability.

EMPLOYEES - AVOIDING THE THREAT FROM WITHIN

Problems that are caused by unscrupulous or uninformed employees continue to rear their ugly head.

Unscrupulous employees

Three factors stand out as to why unscrupulous employees commit fraud and cyber crime:

- **Opportunity:** this usually occurs as a result of weak internal controls which allow a fraudster or cyber criminal to believe that they will not get caught.
- **Motive:** while greed is the most obvious motivation, there are many reasons why fraud and cyber crime occur. Fraudsters and cyber criminals may require money in order to finance lavish lifestyles or feed an addiction. Employees may also be trying, by any means, to meet a financial target.
- **Rationalisation:** an employee may justify the action which has been, or is just about to be taken, by convincing themselves that they are owed the remuneration by the employer.

To combat employee fraud and cyber crime, advice can be sought on profiling employees and third parties. In June 2007 it was reported that Lloyds TSB had gone a step further and purchased a pattern-recognition software system which would enable it to go some way towards detecting employee fraud within its retail banking operation. This type of software is common for spotting fraud in external transactions such as credit card spending. However, Lloyds TSB is the first UK retail bank to purchase the software in order to monitor its employees.

Uninformed employees

Although less sinister, the losses which may flow from an uninformed employee are no less serious.

Employees who are unaware of the potential damage which may be caused by a stolen laptop or working

from home on a computer with inadequate security can expose businesses to third-party losses.

Uninformed employees are somewhat easier to manage than those who are unscrupulous. The key is to ensure that all employees are:

- **Aware** of company policies in relation to the removal of confidential information from the workplace and which information may be sent via e-mail and over the internet.
- **Supported** should they choose to blow the whistle on any wrongdoing they have identified. Companies should ensure that employees do not fear that their jobs will be put at risk if they expose wrongdoing. This may be partly achieved through the provision of confidential and anonymous methods of reporting wrongdoing.
- **Educated** as to where and how cyber crimes can occur, areas of vulnerability within a company and its systems and what their role is in preventing unauthorised access to confidential information. A proactive approach to cyber security is essential. Employees failing to exercise due care and attention can open up their company to fraudsters and cyber criminals. A tick-box mentality can be fatal to a company's security; there is a need to remain vigilant to possible threats at all times.

INVESTIGATIONS

Carrying out prompt, effective and, more importantly, legal investigations into reports or suspicions of cyber crime taking place can help to reduce potential losses and liability for the losses of others.

The primary focus in this area must be awareness: of the law; of third-party rights; of actions likely to be taken by employees or external contractors; and of the type of information obtained.

The cases cited in our article on the risks of self-help remedies in cyber crime investigations (*L v L and another* and *Dubai Aluminium Co Ltd v Al Alawi and others*, *IHL149*, p56) highlighted the pitfalls which may await those who are trying to investigate wrongdoing by others. In both cases cited, as well as in the Hewlett Packard example mentioned in the article, problems arose as a result of actions by third parties employed to undertake investigations.

The cases provide a stark warning. Not only must companies ensure that they are aware of current law, they must also ensure that those they employ to undertake investigations on their behalf are aware of it, and abide by it.

The importance of this awareness was demonstrated in August 2007 when it was reported that a group of reporters and their families affected by the pre-texting scandal (to which reference was also made in *IHL149*) had sued Hewlett Packard for an invasion of their privacy, which caused emotional distress. Hewlett Packard, which has already paid \$14.5m to settle civil claims as a result of the scandal, now faces demands for undisclosed damages.

An additional concern when undertaking investigations is that criminal sanctions may be taken against those who breach sections of the Data Protection Act 1998 and the Regulation of Investigatory Powers Act 2000. It would be prudent, in these circumstances, to obtain advice from a lawyer specialising in this area before embarking on any self-help remedies. Where it is decided that an investigation is to be undertaken, it is also necessary to make stringent checks of the methods used by those employed externally to ensure that they abide by the relevant regulations.

HOW TO AVOID BEING LIABLE AS A THIRD PARTY

Unfortunately, no system within a company is infallible and it is therefore a false comfort to rely on the maxim of 'it will not happen to me'. Effective protocols and their rigorous implementation and testing not only help to avoid problems arising in the first place, they may also reduce liability for any losses caused by problems which have already arisen.

As with carrying out lawful investigations, one of the keys to avoiding becoming liable as a third party is awareness of the law and of the actions of others. Also, effective monitoring – particularly of the company website – as well as protocols for a swift and well-organised response to reports of potential problems can reduce liability.

Awareness of the law and an effective and swift response is particularly important for avoiding or reducing liability under the Data Protection Act and becoming vicariously liable for misuse or breach of a company's computer.

Although there is no law in the UK requiring that companies inform customers or clients about security breaches, as there is in California, such a

law has come a step closer. In August 2007, a report called *Personal Internet Security* was published by the House of Lords' Select Committee on Science and Technology. The report calls for a data security breach notification law which it argues 'would be among the most important advances that the United Kingdom could make in promoting personal internet security' (Chapter 8, para 8.18).

Where there has been a security breach, it is important that companies fully appreciate that how they react may have a very significant impact on the damage done to them. Putting reputation above responsibility can have serious consequences.

By way of example, if a company that holds details of 1 million credit cards discovers that there has been some form of unauthorised access exposing the details of 10,000 cards, it may consider the appropriate course of action is to take no action. However such a loss can rapidly escalate if it then transpires that details of those cards have been sold to a criminal and £100 has been spent on each one of them, the company faces a claim for a minimum of £1m, even before the banks bring a claim for the replacement costs they incur. If the loss then becomes public, the damage done to the company may be catastrophic, not only in terms of existing customers, but also potential customers and suppliers who do not trust a company that covered up the unauthorised access.

In these circumstances, companies need to react in a prompt and appropriate manner to system breaches. Just as happens when food (or, more recently, toys) are found to be unsafe, it may well be that consumers regard an announcement regarding a breach of security and the steps being taken to rectify it as the actions of a company that looks after their interests.

LIABILITY FOR DUTIES OWED TO THIRD PARTIES – CONSTRUCTIVE TRUSTS

Liability stemming from the inadvertent creation of a constructive trust can be avoided by ensuring that those involved are aware of the steps they must take.

Knowing receipt and dishonest assistance

The key words here are 'knowing' and 'dishonest'. Liability stems from knowingly receiving property which has been disposed of in breach of a fiduciary duty, or dishonestly assisting a third party in breach of a fiduciary duty. If adequate checks and enquiries are carried out, the risk of liability can be significantly reduced. A company may need specialised advice on the extent of the checks and enquiries required.

The knowledge required in this area is actual knowledge, and liability can stem from wilfully or recklessly avoiding obtaining such knowledge.

'Where there has been a security breach, it is important that companies fully appreciate that how they react may have a very significant impact on the damage done to them.'

Dishonesty is judged objectively for the purposes of establishing dishonest assistance.

If employees are to make adequate enquiries and checks, they will need to know that the culture of the company does not involve shutting one's eyes to the obvious. If an employee becomes aware of a potential breach of a fiduciary duty by a valued customer, they should feel that they will be supported if it is reported. Whilst this could result in the loss of a valued customer, there are benefits. Employees will see that fraud is not tolerated – a fraud may be uncovered involving the customer which demonstrates that it is not as valued as first thought – and it limits the possibility of third-party claims being brought against the company.

CONCLUSIONS

To avoid becoming a victim of cyber crime, or liability as a third-party, it is clear that potential risks must be identified. Once this is done, effective protocols must be adopted and applied to counteract the risks.

Protocols are only effective if all relevant individuals are aware of them and aware of their responsibilities under them. They also need to be enforced, as well as regularly tested and updated.

Employees must be sure that they will be supported and that reports made by them of wrongdoing or system vulnerabilities will be acted upon. This will encourage a proactive and responsible culture that will filter throughout the organisation.

Managers should be provided with adequate information regarding their responsibilities. These can stretch from knowing how confidential information is stored and handled within the company, to the content of e-mails sent from the company system, to ensuring staff make adequate enquiries of customers and the origin of their assets.

Despite the fast pace of development in this computer age, the importance attached to being aware of risks, rights and responsibilities cannot be overstated. Ignorance is never an excuse.

By Anthony Riem, partner, and Lucy Hamilton-James, solicitor, international fraud and commercial litigation, PCB Litigation LLP.

*e-mail: ajr@pcblitigation.com,
lhj@pcblitigation.com.*

*Tel: +44 (0)20 7831 2691.
www.pcblitigation.com.*

L v L and another [2007] EWHC 140 QB

Dubai Aluminium Co Ltd v Al Alawi and others [1999] 1 All ER 703