

Quarter in law

Welcome to the spring edition of our newsletter. Please click on the links to read about the latest legal issues affecting business.

The weakest link – data security and people issues

2007 has been called the year of the data breach, with a number of well-publicised losses of personal data by public bodies and record fines from the Financial Services Authority... [click here](#)

Database rights – plugging the hole in claiming breach of confidentiality

A recent High Court decision has held that ex-employees who copied and retained documents belonging to their former employer were infringing database rights and had breached their obligation of fidelity... [click here](#)

The Walker guidelines

In November 2007, Sir David Walker, chairman of the British Private Equity and Venture Capital Association (BCVA) working group on disclosures published the finalised *Guidelines for Disclosure and Transparency in Private Equity*... [click here](#)

Intellectual property rights holders to use information from public authorities in civil proceedings

In October 2007, a statutory instrument came into force setting out the circumstances in which rights holders may be able to use information they have obtained from public bodies to bring civil proceedings against potential infringers... [click here](#)

Tax appeal reform

The Tribunal Service (an executive agency of the Ministry of Justice) has recently published a consultation paper setting out its proposals for implementing part 1 of the Tribunals, Courts and Enforcement Act 2007... [click here](#)

The immigration revolution – registering as a sponsor under Tier 2 of the points based system

Tier 2 will replace the current work permit system and any organisation wishing to employ non-EEA nationals must register as a sponsor... [click here](#)

The weakest link – data security and people issues

2007 has been called the year of the data breach, with a number of well-publicised losses of personal data by public bodies and record fines from the Financial Services Authority (FSA).

Big risks for recruitment sites

The recent hacking attack on a major online job search website highlights the risks for any online service – and recruitment sites in particular. 1.6 million data entries, relating to hundreds of thousands of users registered on the site, were found on a server in the Ukraine. It emerged that hackers used a Trojan to access the recruiter section of the site and extract personal details of candidates including names, contact addresses, telephone numbers and CVs. The Trojan was also used to send spam and phishing emails.

This story should prompt any provider of online recruitment or web-based managed services to review its information security. Adequate security measures are one of the key requirements of UK data protection law. This means that the current security environment must be taken into account, so examples of attacks like this cannot be ignored as one-off events affecting someone else. Password systems, as well as staff access rights, may also need to be reviewed to reduce the risk of password theft and unauthorised access.

The issue goes beyond legal obligations. In light of recent breaches, suppliers would be wise to review the information they require from candidates to minimise any data that can be exploited by hackers. Users could also be guided on how to reduce their exposure; for example, not to upload exploitable or sensitive information or to make sure they use discardable email addresses rather than permanent ones. An action plan for data breaches should be in place, identifying when customers are to be notified and what immediate steps they need to take to protect themselves.

Data risks of temporary staff

A recent survey of 100 temporary workers by Websense, a web security company, produced some worrying results: 88% of temporary staff had the same access to documents on the company system as permanent staff; 62% had used someone else's log in details; and 42% were able to connect a personal USB device, such as an MP3 player or memory stick, to their work computer. Such flaws expose businesses to information leakage either by mistake or malicious intent. These businesses are also breaching data protection law by failing to have adequate security measures and access controls in place. Temporary staff and agency workers are an obvious risk because they may not be subject to the same training, vetting and other controls as permanent staff.

It is important to note that most of the recent high profile breaches occurred because of employee action as opposed to IT systems attacks. Proper data management controls covering both permanent and temporary staff are essential to reduce the risk of breaches on the ground, and this is an issue for HR managers as much as for IT departments.

Agencies on the hook

This is also a good time for suppliers of agency workers to consider if they are at risk from the errant actions of their workers. Agencies are likely to be on the hook for data breaches by their workers particularly where the client contract imposes obligations of confidentiality.

Agencies must review their risk exposure and how it can be reduced.

Cont'd

The weakest link – data security and people issues, cont'd

Social networking sites and Web 2.0

According to Websense, 81% of respondents had unlimited internet access from their work PC, 67% used social networking sites and 26% accessed download sites from their work PC. This is not just a worry for temporary staff. The issue is that social networking and new web services expose companies' IT systems, confidential information and intellectual property to an unprecedented extent.

The privacy concerns around the use of social networking sites are obvious, given the degree of personal information typical users divulge. Users who access these and other Web 2.0 sites also increase the probability of attacks on the corporate IT system and data leakage because of the degree of content downloads, peer-to-peer interaction and self-publishing made possible through these sites. Yet most companies, while allowing personal email and internet use, do not block access to such sites or make it clear that these sites must not be used.

The cost of data breaches

What is the size of the risk? While the fines meted out by the UK Information Commissioner have so far been relatively small, recent FSA fines show that financial institutions should certainly not be complacent. But the real cost of data breaches goes beyond fines, potential liability for directors or even bad publicity.

There have been attempts to quantify the costs. Research by the Ponemon Institute in the US which surveyed 35 organisations that suffered data breaches found that the average cost of a data breach per customer record was \$197 in 2007. The average total cost per company was more than \$6 million. Lost business opportunity accounted for 65% of the losses, while the rest included legal costs and costs of remedying IT systems. Loss of customers is a significant factor: according to the Privacy Rights Clearinghouse in its National Survey on Data Security Breach Notification, about 23 million adults in the US were notified of lost or compromised data of which 20% terminated their accounts immediately. Another set of figures comes from a major security breach suffered by a US-based retailer, which has revealed costs of around \$256 million in battening down IT systems and settling class actions from banks for the costs of replacing customer credit cards.

The 2006 Department of Trade and Industry (now the DBERR) Information Security Breaches Survey, suggested that the overall cost of security breaches to UK plc was in the order of £10 billion per annum. The average cost for the worst incident for large companies in 2006 was £90,000. The US figures may be impacted by some very large instances and the prevalence of class action law suits, but even the UK figures are likely to be significantly higher now compared to 2006 – in the millions of pounds for some of the high profile examples.

Of course the statistics do not describe all the pain, including management and staff time and long-term business impact, which are all hard to quantify.

What should be done?

An organisation's data vulnerabilities can easily fall between the gaps – data security is often perceived as being the responsibility of the IT department, yet the IT department may not be best placed to understand all the people risks. HR professionals need to play their part in defining where the responsibility lies, reviewing processes and management controls and verifying that staff are complying on the ground.

denis.potemkin@pwclegal.co.uk

Database rights – plugging the hole in claiming breach of confidentiality

A recent High Court decision (*Crowson Fabrics Ltd v Rider & Ors* [2007] EWCH 2942 (Ch)) has held that ex-employees who copied and retained documents belonging to their former employer were infringing database rights and had breached their obligation of fidelity.

Crowson Fabrics Limited was engaged in the design, production and supply of fabrics for home and furnishing decoration. The company's former employees left the company in June 2007 to set up a new fabric business known as Concept Textiles Limited. The former employees did not inform their employer that they intended to set up a rival business when they gave their notice.

The former employees were not subject to any restrictive covenants or express contractual duties of confidentiality.

As the information was already in the public domain, the former employees could not be prevented from using the information or material based on its confidentiality. The court said an ex-employee could not be prevented from using their skills and expertise that they had built up over a period of time. If an individual can recall the materials and information from their employment, then it could be used after they leave.

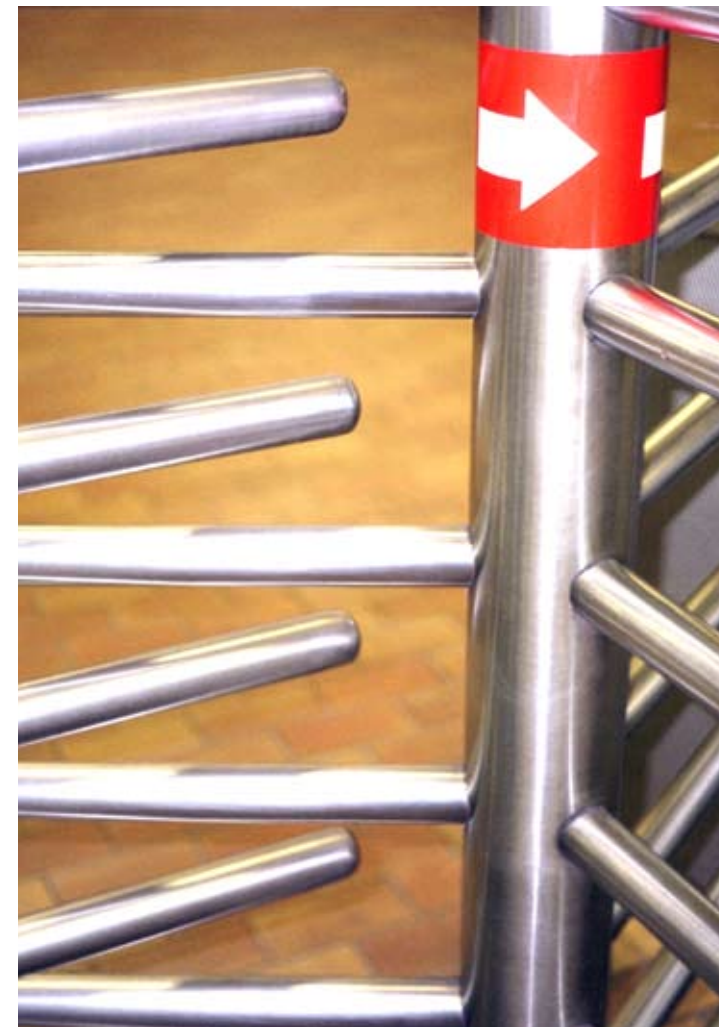
Although there was no breach of confidence, the former employees had not made legitimate use of the information which they were actively using to set up a competing business before they had left their employer.

By doing this, they had breached their duties of fidelity owed to their employer. Since one of them had held a senior position, he had also breached the fiduciary duty he owed to the company while he was employed.

The court also found that there had been a substantial extraction from the company's database of information into Concept's computer system. For example, a spreadsheet created by the defendants listed 3,500 of the company's customers ranked in order of 2007 sales, with figures for each customer from 2006 and 2007 (before the termination of employment). The former employees also sent a list of more than 70 email addresses from the company to the Concept email account. Extracting the information in this way was, the court said, an infringement of the company's database rights. Interestingly, the court readily found there had been sufficient investment in the creation of the databases to earn protection. This was in spite of the tests introduced by recent database case law, after which it was feared many databases would no longer qualify.

This case should remind employers of the potential for database (or other intellectual property) infringement claims and cases based on the non-contractual duties owed by employees, even when a breach of contract and breach of confidentiality claim are not possible.

purabi.chatterjee@pwclegal.co.uk



The Walker guidelines

In November 2007, Sir David Walker, chairman of the British Private Equity and Venture Capital Association (BVCA) working group on disclosure published the finalised *Guidelines for Disclosure and Transparency in Private Equity*. This document is the result of a consultation process which began in July 2007, aimed at investigating the most efficient means to stem perceptions from interested parties and the public at large that private equity is overly secretive and, in some cases, focused on short-term value stripping rather than long-term growth.

The guidelines are limited to cover private equity firms managing large portfolio companies (broadly public companies over £300m or private companies over £500m, generating 50% of revenues in the UK and with in excess of 1,000 employees in the UK). Rather than impose strict rules, the objective is to establish clearer guidance to benchmark the quantity and quality of information large private equity groups publish, thereby increasing their engagement with stakeholders. Key measures include:

- enhanced reporting from portfolio companies within six months of their accounting year end, including details of the controlling private equity funds, the senior managers or advisers of the funds managing the companies and their boards;
- a quoted company style business review, including forward looking statements analysing factors likely to affect the future of the business, including industrial relations, environmental and social issues;

- a financial review including risk management and leverage information; and
- ongoing data provision to the BVCA to assist it in carrying out its strengthened monitoring and reporting functions.

The private equity firms themselves must also provide details of their structure, portfolio of investments, strategy and generic information about their investors.

The BVCA is responsible for keeping the guidelines updated, as well as collating the information produced. The aim is to enhance the BVCA's ability to adequately represent large buy-out firms, and improve their image in the public eye.

Only time will tell if the guidelines improve the relationship of private equity with their employees and the public. The recent credit crunch may have deflected the public's attention away from private equity but several major exits this year could draw interest back and this increased openness may be tested.

The guidelines may be a step in the right direction towards engaging private equity with a wider audience, but they may not be enough to stem further public pressure for other types of fund or put sufficient pressure on overseas investors to adopt greater standards of transparency if they want to do deals in the UK.

laura.cox@pwclegal.co.uk



Intellectual property rights holders able to use information from public authorities in civil proceedings



Until recently, intellectual property rights holders have been prohibited from using information they have obtained from public bodies to bring civil proceedings against potential infringers. This has been particularly frustrating for brand owners who often liaise with Trading Standards officials and HMRC to determine whether goods are counterfeit.

On 1 October 2007, a statutory instrument came into force setting out the circumstances in which rights holders may be able to use such information according to section 241A of the Enterprise Act 2002.

The Act imposes restrictions on the disclosure of information held by a public authority relating to the affairs of an individual or business. However, under section 241A, a public authority is entitled to disclose prescribed information to any person:

- for the purposes of, or in connection with, prescribed civil proceedings (including prospective proceedings) in the UK or elsewhere; or
- for the purposes of obtaining legal advice in relation to such proceedings; or
- otherwise for the purposes of establishing, enforcing or defending legal rights that are, or may be, the subject of such proceedings.

The statutory instrument 'prescribed information' includes information that comes to a public authority in connection with the exercise of any function it has under, or by virtue of specified enactments, including many on which Trading Standards rely to bring criminal proceedings against alleged infringers. Prescribed civil proceedings include proceedings relating to the infringement of an intellectual property right and passing off or the misuse of a trade secret.

As a result of this development, IP rights holders may now approach public bodies to obtain information they might be holding about potential infringers for use in civil proceedings. This should ease the financial and administrative burden of identifying infringers and enable rights holders to bring civil proceedings against an infringer more quickly.

It should be noted, however, that information disclosed by HMRC still can not be used in connection with civil proceedings: the enactments specified by the statutory instrument did not include the regulations which govern the disclosure of details of potential infringers by HMRC and the limited circumstances in which such information may be used.

hannah.shield@pwclegal.co.uk

Tax appeal reform

The Tribunal Service (an executive agency of the Ministry of Justice) has recently published a consultation paper setting out its proposals for implementing part 1 of the Tribunals, Courts and Enforcement Act 2007. The Act overhauls the current tribunal system by creating a new two-tier tribunal service; the First-tier Tribunal and the Upper Tribunal into which most existing tribunal jurisdictions (including those for tax) will be transferred. In tax, the reform seeks to create a unified appeals system for direct and indirect tax disputes to reflect the merger between the Inland Revenue and HM Customs & Excise in 2005.

Current tax appeal tribunals

There are currently four tribunals hearing appeals against decisions made by HMRC. These are set out below.

General commissioners of income tax

The general commissioners are lay people who hear straightforward appeals against HMRC direct tax decisions. There are around 2,000 general commissioners spread across the UK. They are supported by clerks (usually solicitors) who provide administrative support and legal advice.

Commissioners for the special purposes of the Income Tax Act

The special commissioners deal with appeals in more difficult direct tax cases and are legally qualified. There are 25 special commissioners who cover the whole of the UK, although most hearings are held in London.

VAT and Duties Tribunal

This tribunal hears appeals against HMRC's indirect tax decisions. There are 35 legally qualified chairmen and 87 part-time lay members. The 25 special commissioners also sit as chairmen of this tribunal. There are three main hearing centres: London, Manchester and Edinburgh.

The Section 706 Tribunal

This tribunal only considers appeals relating to anti-avoidance provisions. It meets infrequently and its members are appointed by the Lord Chancellor.

The new system

The First-tier Tribunal will be the first instance forum for most cases. It will be large, with approximately 190 judges and 3,600 lay members covering issues from benefit entitlement and special educational needs to alleged carousel VAT fraud. It will be divided into specialist chambers to ensure that the proper degree of judicial expertise and knowledge is brought to bear on cases. Each chamber will have a president, whose role is to maintain and improve the chamber's expertise. The president will also be a judge of the Upper Tribunal. Five chambers are proposed, one of which will deal with taxation.

The Upper Tribunal will be a dedicated appeal body at the head of the new system. Its authority will derive from its specialist skills and its status as a superior court of

record with judicial review powers. It is expected that the Upper Tribunal will come to play a central role in the new system, enjoying a position in the judicial hierarchy at least equivalent to that of the administrative division of the High Court. Appeals from the Upper Tribunal will be to the Court of Appeal with permission (only in cases of general importance or for other special reason).

The Upper Tribunal will be divided into three chambers, of which one will be finance and tax.

The upper finance and tax chamber will become the appeal body for the First-tier taxation chamber and will take over the present appellate function of the chancery division. High Court judges from the chancery division are expected to sit in the Upper Tribunal chamber, not only to enhance the Upper Tribunal's status, but also to ensure the exchange of expertise in finance and tax matters, which will feed through to the courts. Most of the authoritative guidance will come from the Upper Tribunal because of its size and composition.

[Cont'd](#)

Tax appeal reform, cont'd

How will the new system work?

The proposed structure is designed to ensure a close working relationship and good lines of communication between the Upper Tribunal and the First-tier Tribunal. A key issue in moving to the new tribunals system will be to ensure that the new system is flexible. The Government recognises that a large number of tax cases are on simple points and do not require determination by someone legally qualified. Consequently, it sees a continued role for non-legally qualified individuals within the new system. The Government also sees it as a priority that the more complex or sensitive cases are identified quickly so that they can be dealt with appropriately.

It is envisaged that most cases will go initially to the First-tier Tribunal, with an onward appeal to the Upper Tribunal only with permission and normally on a point of law. Only a few cases will be heard by the Upper Tribunal as a first instance court. These include group litigation cases and lead cases. Taxpayers may request that their case be heard directly by the Upper Tribunal where it gives rise to an important point of law or where it is “likely to reach the Court of Appeal in any event.”

Timing

It is proposed that the relevant tribunals be transferred to the new tribunal service after April 2009. HMRC is considering proposals for transition to the new system.

boaz.goren@pwclegal.co.uk



The immigration revolution – registering as a sponsor under Tier 2 of the points based system

Considerations for prospective sponsors

Tier 2 of the new points based system (PBS) will replace the current work permit system. Under the new system, any organisation wishing to employ non-European Economic Area (EEA) nationals must register as a sponsor. There are certain considerations which must be taken into account before an employer can register.

When a sponsor comprises of more than one legal entity, it can apply for either a collective licence covering the group or a separate licence for each entity. There are distinct advantages to both options, the former offering more central control to the sponsor's immigration operations and the latter safeguarding the other entities from being downgraded in the event of non-compliance by an individual entity.

It is likely that the sponsor will have to state the number of potential Tier 2 applications it will make. It is important that this estimate is accurate as the sponsor may have to justify its number. Additionally, the Government's November 2007 Statement of Intent (Sponsorship under the Points Based System) states that there will be review thresholds (i.e. a specific number, identified by the BIA, whereby the sponsor's immigration activity will be reviewed). The number of potential Tier 2 applications stated could feed into the review threshold.

Sponsors must have a complete idea of how many non-EEA nationals they employ in the UK, and have sufficient processes to ensure compliance. This will include ensuring:

- the sponsor has a record of the employee's immigration status;
- the employee informs the sponsor of any changes in their status; and
- procedures are sufficiently aligned to ensure the status of each employee is compliant from an immigration and tax perspective. This will be particularly important for those employees in the UK under short term business visitor agreements.

In common with the current system, sponsors will be able to appoint a representative to advise and assist with registering and future applications under Tier 2. All sponsors must gather and verify all the necessary documentation for registration.

The application process

The licence application must initially be made online. The process requires a company to identify their main contacts for immigration purposes and their immigration representative. It is likely that all supporting documentation, including audited accounts, must be submitted in hard copy within 14 days of making the online application. The application will then be considered by the BIA who will assess the company's set-up and its readiness for PBS.

The immigration revolution – registering as a sponsor under Tier 2 of the points based system, cont'd

Upon approval

After the application is approved by the BIA, the employer can be a sponsor. Sponsors will be divided into A and B ratings, depending on their past record of compliance with immigration rules, and whether the likely compliance of the entity going forward is reliable. Each sponsor will be publicly listed on the Sponsor Register and will also be granted access to the web-based sponsor management system.

The sponsor can then issue certificates of sponsorship to any non-EEA national it wishes to employ under Tier 2, provided they meet the criteria for sponsorship. However, together with greater control of whom it employs, the sponsor will be required to adhere to greater compliance obligations. The sponsor must, to the best of its knowledge, ensure that a migrant is legally entitled to work and (if applicable) has the appropriate registration to work.

Sponsors found to be in breach of their sponsorship duties may receive an educational visit to their premises which may result in:

- the implementation of an action plan:
- a written warning for employing an illegal worker: and
- a down-grading on the PBS sponsorship register; removal from the PBS sponsorship register, or civil or criminal penalties.

Employers will still be able to employ the most highly skilled under Tier 1, which replaces the current highly skilled migrant programme.

anjali.raman@pwclegal.co.uk

Tier	Type of worker	Implementation
Tier 1	Highly skilled migrants such as professional graduates and entrepreneurs. This will be similar to the current highly skilled migrant programme visa. Applicants with this visa can work for any UK employer	April 2008
Tier 2	Skilled workers with a job offer who do not qualify under tier 1	October 2008
Tier 3	Workers to fill low skilled shortage occupations	October 2008
Tier 4	Students applying to study in the UK	April 2009
Tier 5	Temporary workers such as visiting workers, youth mobility and cultural exchange and selective development schemes	October 2008

This publication has been prepared for general guidance on matters of interest only, and does not constitute professional advice. You should not act upon the information contained in this publication without obtaining specific professional advice. No representation or warranty (express or implied) is given as to the accuracy or completeness of the information contained in this publication, and, to the extent permitted by law, PricewaterhouseCoopers Legal LLP, its members, employees and agents accept no liability, and disclaim all responsibility, for the consequences of you or anyone else acting, or refraining to act, in reliance on the information contained in this publication or for any decision based on it.