pitmans
MAKING IT HUMANLY POSSIBLE

Ex-Employees & Confidential Information - What Rights Do Employers Have?

In F1, Force India experienced a sinking feeling when its Chief Technology Officer, Mike Gascoyne, left to take up the same role at Lotus. Force India issued UK civil proceedings against Gascoyne and others in June 2010 for "a very serious breach of intellectual property". In response, Gascoyne has stated:

> "Obviously our wind-tunnel model was designed for us by Fondtech in Italy...It is based around a 2010 chassis, because there is a big fuel volume in it, it has a Cosworth engine, an Xtrac gearbox, our suspension, and other stuff designed by us. The Fondmetal guys put some generic bodywork on.....Whereas you cannot copy anything or take anyone else's IP you can use your expertise and you will base that on what you know and what directions you know have been happening. That is what has happened."

In the automotive industry where employees are likely to switch to a competitor, employers need to know what information ex-employees are allowed to take and how they can limit the potential damage to their business.

Identifying Different Types of Information:

There are four types of information used in a business. These are (1) trade secrets, (2) other confidential information which is of such a high degree of confidentiality that it amounts to a trade secret, (3) employee's skill and knowledge and (4) information in the public domain.

Information can be classified as a trade secret if it allows a business to obtain an economic advantage over its competitors and it is not in the public domain. Examples of trade secrets can include secret processes of manufacture such as formulae, designs, special methods of construction, manufacturing processes, business plans and methods, financial or statistical information, customer lists and databases, computer source code, plans and technical drawings.

For public policy reasons, an employee is allowed to use all his acquired skill and knowledge no matter where he acquired it from and whether or not it was secret. It is seldom an easy question to resolve what is and what is not an employee's skill and knowledge. The more complex the information, the more likely that it has not become part of an employee's existing knowledge and skill.

There has been a distinction between general background information and information deliberately memorised in order to be used elsewhere. If evidence can be produced that the information had been deliberately memorised it will not come under the definition of an employee's own skill and knowledge.

Breach of Post-Termination Restrictive Covenants and Breach of Confidentiality:

A claim for breach of confidentiality will usually be brought in addition to a claim for breach of restrictive covenants.

Trade secrets and other confidential information which is of such a high degree of confidentiality that it amounts to a trade secret can be protected by well drafted restrictive covenants in employment contracts and a claim for breach of confidential information. Restrictive covenants protect trade connections and goodwill as well. It is of the utmost importance that these are

carefully drafted by an employment lawyer as they will be void and unenforceable if drafted too widely or for too long.

Information which forms part of an employee's skill and knowledge and public domain information cannot be protected under these two actions. The case of *Faccenda Chicken v Fowler* [1986] makes it clear that once an employee has left employment only trade secrets or similar highly confidential information is protectable.

Misuse of confidential information is the most difficult part of any breach of confidence action and this is one reason why pre-emptive strikes such as search and seizure orders, disclosure, delivery up and interim injunctions are commonly employed. However, pre-emptive strikes are expensive and it is a commercial decision on the facts of each case as to whether they might be appropriate.

As the disclosure or continued misuse of confidential information can destroy the very thing a claimant is attempting to protect, the most practical remedy available to an employer is often to obtain a swift interim injunction that will last until the matter is dealt with by a court or resolved.

The scope of an interim injunction may be limited by time and place. It may restrict only certain activities and last only until the relevant information is no longer secret or until the conclusion of legal proceedings. However, if a claimant's case is successful, they are also able to seek a permanent injunction to provide an ongoing prohibition on the misuse of the confidential information beyond the conclusion of the case.

Database Right Infringement:

As the above two actions give the ex-employer little protection, employers have started to use a new type of action to recover damage caused by leaked databases.

The Database Directive (96/9/EC) introduced a database right which protects the compilation of information making up the database. A database right will automatically exist where there has been a "substantial investment" in obtaining, verifying, or presenting the contents of the database. At least one of the database makers must be from the EEA.

An employee is likely to infringe a database right if he takes customer lists with him when he leaves and subsequently uses the information for his own benefit (re-utilisation). The fact that the employer does not have to prove that the contents of the database are confidential means that database right is a more straightforward and cheaper cause of action than breach of confidence.

In the case of C*rowson Fabrics Ltd v Rider* [2008] ex-employees copied and retained various documents belonging to their ex-employer including customer contact details and sales figures. The high court held that the ex-employees had not acted in breach of confidence as the information was either in the public domain or within their gathered skills and expertise so that it was not confidential. However, the ex-employees had infringed their ex-employer's database rights by copying various customer sales figures and electronic files from its computer system.

Other Intellectual Property Right Claims:

The unauthorised use of patents, copyright, design right and trade mark rights will generally infringe the respective right. This will potentially entitle the owner of the right to bring a claim seeking an injunction to prevent all further use and to recover compensation and costs. In addition, rights may be lost as a result of leaks in confidential information.

Employers should review their contracts with consultants, employees, contractors and agents to ensure that the company owns all of the IP created by them under each agreement. Generally, in the absence of an appropriate agreement, IP created by a non-employee will not be owned by the company.

What Can a Business Do to Prevent a Leak of Confidential Information?

The nature of confidential information is such that misuse of it has the effect of destroying its value by compromising its confidentiality, so prevention is key.

Agreements

A well drafted confidentiality agreement is particularly valuable in situations involving departing employees, customers and suppliers. It is also worth ensuring that third parties such as suppliers and distributors have in place contracts expressly providing for some form of recourse if they disclose confidential information or trade secrets.

Employers should include effective clauses in employment contracts covering restrictive covenants, garden leave, confidentiality and ownership of Intellectual Property Rights.

Computer security

In the age where trade secrets and other confidential information of most businesses are held in digital form it is easy for employees who are leaving to join a competitor or set up a rival business to download vast quantities of data onto disks or memory sticks, and simply walk out the door. Or they may prefer to e-mail the information to a personal account and consider it at leisure in the comfort of their own home.

Employers should try to use the computer systems to their advantage by planting seeds (fake entries) into databases and using a document management system to track records of when documents have been accessed, by whom and whether it has been copied. Both of these will make tracking copying easier to evidence.

Keeping records considerably strengthens most claims as it is all based on evidence. Recording evidence such as time and resources that go into creation of a database and of when and by whom copyright works are created will strengthen some of the above claims. Forensic IT investigators can extract the relevant information however they come at a price and are usually part of the team once there is a good reason to believe that information has been taken.

Consider if your IT system can offer greater protection e.g. password access to documents or databases only.

Company Policies

Employers should ensure that the company policy is up to date and deals with confidential information. Make it clear what may be stored and who owns the information and emphasises that employees must keep their personal and business contacts separate. In addition to this it may also be very worthwhile for organisations to provide training to staff and employees on the handling of confidential information and marking documents as confidential where this is the case. In extreme cases it might be worthwhile considering setting up a management program in which the business' key information, including trade secrets, are identified and then placed under in a highly secure location where only authorised personnel are able to access them.

Conclusion:

The digital world has led to an increase in the leak of confidential information. The database right grants employers an exciting wider protection but ensuring you spend the time to put in place preventative measures is crucial. If you are suspicious of a leak, an interim injunction may be able to stop full extent damage being done but you must contact your lawyer as soon as possible.

In the busy automotive industry where time is precious, preventing a leak in confidential information will ensure that precious time is spent innovating new ways to out do competitors and not fighting a legal battle against an ex-employee.

Exactly what action Force India has brought against Mike Gascoyne is uncertain and it will be interesting to see if any further information is released in relation to this. What is certain is that a vast amount of time will have been spent by employees at Force India in relation to various legal battles this year. The costs of which will not be wholly recoverable.

Holly Strube
hstrube@pitmans.com
+44 (0) 118 957 0571