Protecting confidential information in the modern world; an employers' prerogative

September 2017

There are very few businesses that do not have confidential information they want to protect. A database of clients is often the most important information for service companies.

In the modern world where information can be exchanged at the touch of a button, the protection of data is much harder to achieve than it used to be. With the advent of Facebook and LinkedIn non-solicitation clauses have lost their power and employers need to be inventive in finding new ways to protect themselves.

What is confidential information?

Confidential information is very difficult to define; but you know it when you see it. It is best viewed as information that an employer would not want to share with a competitor and could include pricing information and margins, client lists and contacts, details of suppliers, technical information and future business plans.

Information is not confidential if it is in the public domain; so the address of a client is not confidential if it can be found in a phone book or on the internet. However, if an employer has spent time and money putting together a list of clients or potential clients, that list is confidential even if the client details are publicly available and would be protected by copyright laws.

Restrictive covenants

The main way employers can protect themselves against the misuse of confidential information is by restrictive covenants in the employment contract or service agreement. Restrictive covenants are contractual terms that limit what an employee can do while employed and after the end of their employment.

There are four main types of covenant:

1. Non-compete – stops the employee from working in a competing business
2. Non-dealing – the employee can work in a competing business but cannot deal with clients that he or she had contact while working for the previous employer
3. Non-solicitation of clients – the employee can deal with former clients but cannot solicit
4. Non-solicitation of staff – prevents the employee from encouraging other staff to leave and work elsewhere

Restrictive covenants are, by their nature, contrary to public policy because they are in restraint of trade. They are only enforceable if they are no wider than necessary to protect the employer's confidential information and business interests. If they are too wide or too long they will be unenforceable. In a very recent UK case the Court of Appeal struck out a non-compete clause that was too

wide because it prevented the former employee from holding any shares in a competing business. The Court of Appeal was willing to strike down the clause despite the fact that it was theoretically too wide and unlikely to have any actual impact on the ability of the employee to work.

Social media

Historically, a non-solicitation clause would suffice because there was no easy way for an employee to contact all of his former clients. However, in the world of social media not only is contact easy but employees are actively encouraged to connect with all of their clients on LinkedIn and other social media.

When they leave they can update their employment status and post some positive comments about their new employer and all of their former clients will know where they are now working. All of this can be done without any solicitation taking place. Similarly, advertising events for the new employer on social media is not solicitation. However, emails to former clients encouraging them to attend an event may cross the line, as would chat with individual clients encouraging them to move their business.

The reality is that social media has largely rendered the non-solicitation clause ineffective and employers now need non-dealing clauses in their employment contracts. Non-compete is better but has to be very carefully drafted and some employees, particularly senior employees, will baulk at signing a contract that jeopardises their future employment prospects.

Gardening leave

While restrictive covenants offer some level of protection, the best protection is a garden leave clause. This allows the employer to ask the employee to stay at home (on full pay) or undertake alternative duties during his or her notice period. During the period of garden leave the employee is not allowed to contact any clients allowing the employer time to introduce new staff to clients and embed the new relationships.

It is expensive to have an employee sitting at home doing nothing but, in practice, many employers pay in lieu of notice because they are concerned that an employee working his or her notice will be disruptive. If there is a concern that an employee may poach clients or misuse the employer's confidential information put the employee on garden leave for at least some of the notice period rather than pay in lieu.

The ability to put an employee on garden leave needs to be explicitly included in the employment contract.

Avoid the use of personal devices

Previously, it was much easier to control the flow of information because, by and large, information stayed in the office. Of course a determined employee might have a late night session printing out or copying information he or she wants to steal however now it is much easier for employees to email confidential information to their personal email account in the weeks or months before they leave. However this is easy to detect and provides easy evidence for a criminal or civil claim (misuse of personal information can be a criminal offence under the Data Protection Law).

In the modern world employees can often access work data on both work and personal devices. When they leave employment they return the work devices but it is very difficult to enforce the deletion of work information from personal devices. An employee that is allowed to keep his or her work contacts on a personal phone can export those contacts to another device in seconds. It is expensive and time consuming to check that a personal device has been cleaned of all work data.

Employers are forced to rely on employees confirming that they have deleted the data. Such confirmations are unlikely to deter an employee who is determined to use his last employer's data as a foot-up with a new employer. This is especially the case if the employee views the contacts or work product as his or her own work rather than belonging to the employer. Employers that have valuable data should not allow that data to be copied onto personal devices.

Receiving confidential information

It is worth remembering that it is not only the owner of the confidential information that needs to be careful. There are also risks for a receiving business. A business that induces someone to breach confidence or break a restrictive covenant will find itself on the receiving end of a court injunction or a damages claim. It may also have to go through the expensive process of separating out contacts or information wrongly received from its systems or in a worse case scenario a whole database may have to be destroyed.

Businesses should check the restrictive covenants of staff they recruit and require incoming employees to confirm in writing that they will not breach any obligations owed to former employers.

When a new employee turns up with a long list of contacts he or she wants to email to announce their arrival check the source of the data before loading onto your systems.

Our top tips

Here are the top five things employers can do to protect their confidential information:

1. Have a garden leave clause
2. Include non-dealing clauses in the restrictive covenants
3. Do not allow employees to have work data on personal devices
4. Check obligations owed to former employers at the recruitment stage
5. Employees should not be allowed to introduce data onto an employer's systems without the source of the data being checked

If you would like to discuss any of this in more detail, please contact Elena Moran at Collas Crill who can guide you through this process.