EVERSHEDS SUTHERLAND

Prepare and protect

Emerging from COVID and beyond – A guide to protecting your business relationships and confidential information

Click to begin

Introduction

Strong businesses are built on their people, customer relationships, and confidential information.

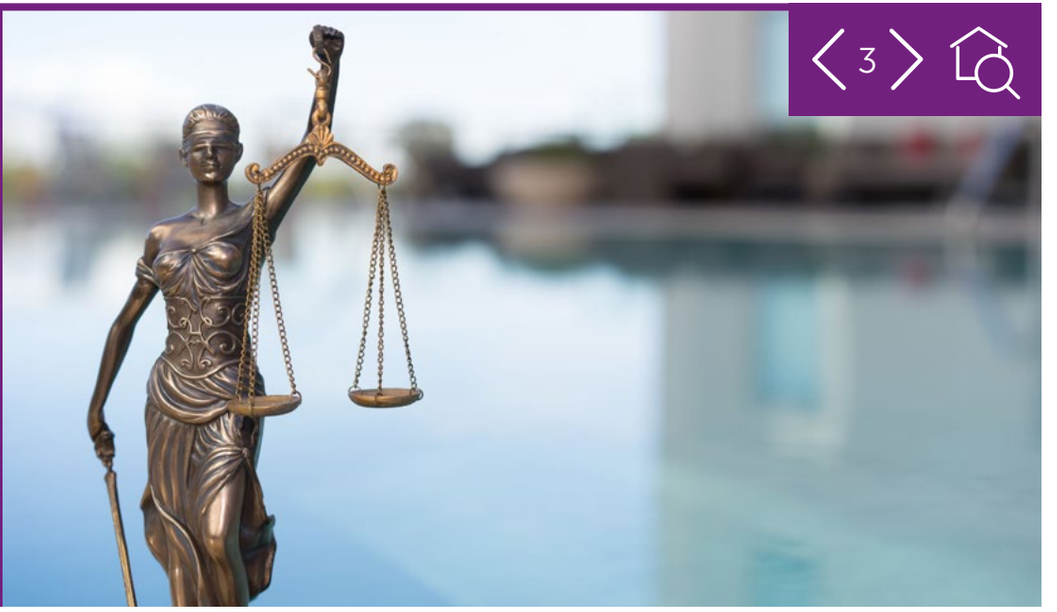
As we emerge from lockdown, employers can expect to see increased movement in the labour market. Employees who have not had the confidence or opportunity to make a career move during lockdown may now be able and willing to take that step, whether that is to go to a competitor or set up on their own. Furlough, reduced hours and redundancy rounds will no doubt have impacted morale and loyalty in some areas.

As such we anticipate that employers are likely in the next few months to need to call on contractual and statutory protections to safeguard their relationships and confidential information. Whilst competition cannot be prevented entirely, a business can put in place all necessary measures to protect itself, and ensure it understands its options should an individual or team depart and seek to operate in a manner which would damage the business. It is important therefore to have up to date enforceable protections in place.

In this guide we provide you with an overview of the following key areas for any business:

- Restrictive covenants and their enforceability
- Garden leave and its impact
- Confidential information protection
- The challenges presented by social media
- The steps to take when a key employee confirms they are leaving
- Enforcing your rights; including:
  - discovery of the issue
  - court proceedings and applications for injunctive relief
  - initial contact
  - options available
  - settlement
- Data privacy considerations

Restrictive covenants and their enforceability



Restrictive covenants may be included in employment contracts in order to protect your confidential information, trade relationships and workforce. Typical covenants seek to prevent an employee, for a certain period following termination of their employment, from:

- working for a competing business
- soliciting key employees
- soliciting customers
- dealing with customers (i.e. not requiring evidence of solicitation)
- dealing with/taking steps to interfere with suppliers

The starting point for the Court is that a restrictive covenant is unenforceable and void as a restraint of trade. However, the Courts are prepared to uphold a restrictive covenant provided it goes **no further than reasonably necessary to protect a legitimate business interest.**

A Court will not re-write a restrictive covenant and therefore it is important to get the drafting right.

There is no set or maximum restrictive period that can be applied – what is enforceable will be considered on a case by case basis, depending on the employee's role, the information and relationships they had access to and what level of threat they would pose if they went to work for a competitor.

For example, it may be reasonably necessary to impose 12-month restrictions on a senior executive who is privy to highly sensitive confidential information (because that is how long the information is likely to remain confidential) and/or who leads key customer relationships (because that is how long it would take the business to secure those relationships). However, this length of restriction may not be appropriate for more junior or mid-level employees. For many employees, a non-compete clause may not be necessary at all, if you could rely on non-solicitation/non-dealing clauses to protect your customer/employee relationships.

Given the above, it is important not to apply blanket restrictive covenants to all employees. You should consider carefully what employees/job roles require restrictive covenants, and then tailor them in each case. Failure to do so is likely to result in the restrictive covenants being unenforceable.

This is important in two respects;

- it will act as a deterrent if the individual seeks advice and is told they are not enforceable
- ultimately you will not have the contractual protection you need in order to take action and protect your business

Restrictive covenants and their enforceability

Common reasons for clauses being unenforceable are:

- non-compete clauses which contain extremely wide geographical restrictions, including areas where the individual never worked
- non-solicitation clauses which refer to all customers, even those with whom the individual never had any contact
- non-solicitation clauses that refer to all employees, instead of employees at a particular level of seniority/in particular roles or teams

In a recent High Court case, an employee had 9 month restrictive covenants, despite also having a probationary period during which only a 2 week notice period applied. The Court held that the restrictions were unenforceable. The employee could have been in employment for a very short time, without having built client relationships, yet would be subjected to lengthy restrictions. Whilst the case was decided on its facts, it does give rise to some concern that where employees have a short notice period during probation, restrictive covenants which apply from day one (which they invariably do) may be unenforceable.

If you need to introduce new restrictive covenants for existing employees, it is necessary to give some consideration to such issues even if the employee signs up to them. For example, it may be advisable to align the introduction of new covenants with a pay rise, promotion or participation in a new bonus scheme. As employees develop and progress through your business it is important to continually evaluate whether the restrictions in their contracts are appropriate or need reusing.

Government Consultation

In February 2021, the UK Government closed a consultation on measures to reform non-compete clauses. Following COVID-19, the Government is 'exploring avenues to unleash innovation, create the conditions for new jobs and increase competition'. There are two key options under consultation:

1. requiring an employer to pay mandatory compensation to the employee during the non-compete period e.g. 60%, 80% or 100% of salary. This is similar to many European jurisdictions; or
2. an outright ban on non-compete clauses (as in California).

Whilst we await the outcome of this consultation, it is clear that the Government is keen to boost the economy and innovation by restricting the use of non-competes, and given the focus on the economic recovery from COVID-19, it is possible that any changes may be introduced relatively quickly.

Garden leave and its impact

Garden leave is a valuable tool. During such period an employee remains subject to the implied terms of good faith and fidelity (despite not being required to work). The longer an individual's notice period, the greater the protection for the business.

In simple terms, it is easier to restrict an individual's activities during a period of garden leave, than it is to try to enforce post termination restrictive covenants.

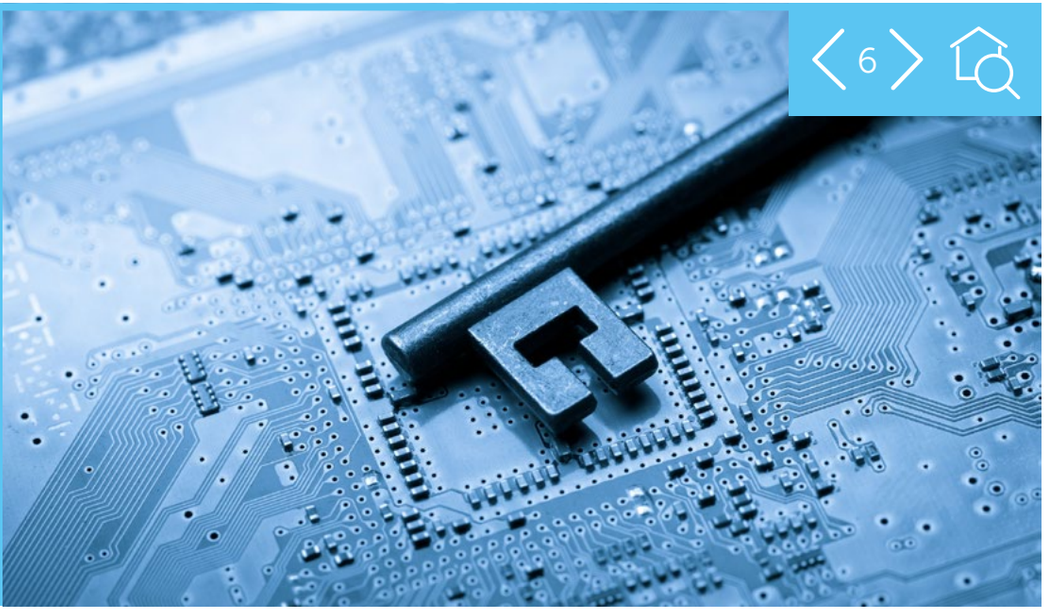
This needs to be balanced with the financial consideration that the employee must receive their normal salary and benefits during a period of garden leave.

Given that a restrictive covenant should go no further than reasonably necessary in protecting the businesses' legitimate interests, Courts often expect any restricted period to be reduced by the length of any time spent on garden leave (and for this to be reflected in the contract drafting). For example, an individual has 12-month restrictive covenants because the employer considers that to be the necessary period to protect its interests. If the individual is then placed on garden leave for 9 months, the length of restrictive covenant should be reduced to three months. Therefore the individual would have been out of the market for 12 months in total – the period the employer originally considered necessary.

It is important, before placing an employee on garden leave or before making a payment in lieu of notice, to check that you have the power to do that in the employment contract. If not, and if you proceed to place them on garden leave and/or pay in lieu of notice, you are technically in breach of contract. Whilst the employee is unlikely to have incurred any financial loss you will not be able to rely on the restrictive covenants in the contract.

For this reason it is also important to ensure that all sums owed to the employee (including any bonus) are paid, to avoid an argument that there has been a breach of contract and therefore the restrictive covenants have fallen away.

Confidential information



Employers understandably wish to prevent the misuse of information that they consider to be confidential, although there is often a lack of understanding about what is capable of protection. There is a difference between what can be protected during and after employment.

There are generally considered to be four categories of information:

- **trade secrets –** only trade secrets can be protected after employment has ended. Examples given by the Courts are secret processes of manufacture (for example chemical formulae/the Coca Cola recipe), designs or special methods of construction, and 'other information which is of a sufficiently high degree of confidentiality as to amount to a trade secret'
- **'mere' confidential information –** this is difficult to define but information which is obviously confidential or which the employee is told is confidential, but which does not amount to a trade secret. This can be protected during employment because the employee has a duty of good faith and fidelity, however it is difficult to protect after employment has ended
- information that amounts to the **general skill and knowledge** of the employee (for example their expertise in a particular field) – this belongs to the individual and can be used as they wish after employment has ended; and
- **publicly available information –** this is not confidential and cannot be protected

This is a much litigated area of law. The leading case is Faccenda Chicken Ltd v Fowler [1984] ICR 589, where a former employee used sales information relating to the requirements of customers and the prices they paid in order to compete with his former employer. The Court held that this was not confidential information akin to a trade secret, and therefore was not capable of protection after employment had ended.

There is often an overlap between confidential information and company property. If an employee has retained a list of customers and contact details, this may not constitute confidential information (as it is not akin to a trade secret) however it is likely to be the employer's property which must be returned (see **Delivery Up Orders** below). That said, it is often difficult to evidence that an employee has retained a customer list/company property, unless there is an electronic trail that they have downloaded, emailed or printed a particular document.

In deciding whether information amounts to a trade secret, the Court will consider the nature of the information itself, where it comes from (for example, has the employer invested significant time and resource in producing it), its purpose and what damage could be caused to the employer if the information was used or disclosed without authorisation.

Whilst it is the Court which will ultimately determine what amounts to a trade secret, it is useful to clearly set out in the employment contract what you consider this to be. The Court will have regard to what you have communicated to the employee and how you have treated that information, including any steps that have been taken to restrict distribution of, or access to, that information (for example database password). marking documents as confidential, using different colored paper and/or monitoring the use of email, photocopiers and other devices (subject to data protection law). From a practical perspective, carefully and specifically drafted clauses in the employment contract may also be an effective deterrent.

The challenges presented by social media

Fast-paced technological advances in recent years have changed the way we do business and interact with customers, but the law has yet to catch up and this poses a challenge for employers.

Employees often use their personal social media accounts in the course of their employment and store contact information there, which remains available to them after termination. As set out above, this information is unlikely to constitute a trade secret (and in any event may be in the public domain, depending on the privacy settings applied) and the extent to which you can argue it is company property is limited. It is unlikely that this information would ever have been stored on your IT system, and usually a social media account is owned and operated by the individual (even if they are using it in the course of their employment).

Furthermore, it is quick and easy for an employee to communicate widely with customers and contacts after termination of their employment, even if they have non solicitation covenants in their contract. They can announce that they have moved on to a new employer (for example by changing the name of their employer on LinkedIn) and provided they don't actually invite customers to contact them, it may be difficult to argue that this amounts to 'solicitation'.

You could consider taking the following steps to protect your business in this regard:

- for key employees, particularly customer facing employees who are likely to use social media accounts in the course of their employment, make it a condition of their employment/an express duty that they maintain and use those accounts for the benefit of the business
- expressly state in the employment contract that the social media account belongs to the employer (this may be more persuasive if you require them to open a new social media account and pay for any 'premium' memberships)
- require them to handover passwords and usernames at any time upon request and in any event when their employment terminates
- require them to keep any lists of contacts on your computer system (see Pennwell Publishing (UK) Ltd v Ornstien [2007] EWHC 1570 (QB)); and
- have a clear social media policy setting out whether employees are permitted to use personal accounts for business purposes and whether they can add business contacts to their own personal accounts

The steps to take when a key employee confirms that they are leaving

It is important to act quickly and decisively when a key employee announces that they are leaving the business. You should develop a process to be followed so that protective steps can be taken without delay. Such steps may include:

- checking the employee's contract of employment to assess whether you have the contractual ability to place them on garden leave
- if they are going on garden leave, instructing the employee not to contact any customers/suppliers/employees
- immediately revoking the employee's IT access/security pass
- arranging for IT (whether internal or external forensic specialists who we can engage on your behalf) to check whether there has been any unusual activity over the previous few weeks - for example emails being sent to personal accounts/downloads of confidential information/documents. We can assist you with this, including providing advice as to the importance of having a well drafted Electronic Information and Communications Policy
- requesting the immediate return of property (including laptops/phones/documents kept in the individual's bag/car)
- remind the employee of their contractual obligations
- from a commercial perspective, consider how to secure customer relationships and/or workforce relationships
- if you need the employee to work their notice:
  - consider whether you can give them work that does not involve exposure to confidential information and/or customers (it may be appropriate to seek legal advice as to whether this can be done without breaching the implied term of trust and confidence, as this could result in the employee leaving immediately and claiming that you have acted in in breach of contract and that any restrictive covenants have fallen away)
  - monitor whether there is any suspicious behavior (such as working outside of their normal working hours/late at night, suspicious IT access, significant amounts of photocopying, requests for business information from finance/secretarial teams, emails to personal email accounts, use of USB sticks)

Enforcing your rights

So far in this guide we have provided you with an overview of the steps you should take to protect your business up until the point of an employee or team departing. We now look at the key considerations and the options available should you find yourself in the worst case scenario - that you suspect that they are acting unlawfully.

Should a restrictive covenant be breached, it gives rise to a claim for damages in the same way any breach of contract would. The same applies in respect of the breaching of confidentiality provisions. You would be entitled to seek damages to reflect the losses suffered as a result of the breach. There are various ways of assessing those losses depending on the nature of, and circumstances surrounding, the breach.

However, by its very nature, a breach of a restrictive covenant and/or the misuse of your confidential information is likely to be a catalyst for serious immediate issues for your business. Furthermore, the longer the breach continues the more likey it is that irreparable damage is done if the unlawful behavior complained of is not stopped. For example if, as a result of such a breach, a valued client was to be persuaded to move its custom elsewhere and is then happy with the services provided, it may be that they are lost to your business for good. Although financial damages would be recoverable, these will not be for an indefinite period.

That being the case, it is important for you to understand the options available and the steps to take to protect your business.

We now look at:

- Discovery of the issue
- Initial contact
- Court proceedings and applications for injunctive relief
- Options available
- Settlement

Discovery of the issue

Following the departure of a key member of your team it would be prudent to, in the first instance, undertake a review of their work email account and electronic workspace in order to check if they have attempted to send emails to their personal email accounts or devices in the lead up to their departure. Similarly if they previously had access to their email account or your network through personal devices then it would be sensible to have both this access blocked, and also to check if any access has been attempted since the date that they departed or were placed on garden leave. We often see examples of where a departing employee has taken action in the days or weeks leading up to them handing in their notice of resignation, so we would suggest considering this when undertaking the above investigations. Should your Electronic Information and Communications Policy allow it, the monitoring of their work email during this period would be sensible.

If your business does not have the IT capability to complete the above checks in-house then we can recommend experts that we work with regularly who can undertake these checks for you.

If the departing employee or team has historically worked with particular clients or accounts and you are confident that you have a trusted long-term relationship with them, then it may also be worthwhile contacting such clients to see if they have been approached.

Often we see situations where the above enquiries generate key evidence of unlawful breaches of restrictive covenants, or the removal and use of commercially sensitive information. It is at this stage where it is sensible to take the matter forward in order stop them in their tracks and protect your business.

Initial contact

In the ordinary course of such matters, following our instruction and an evaluation of the merits of the case, we would normally send a letter before action to the potential defendant(s). This step is required pursuant the pre-action protocol as set out in the Civil Procedure Rules and also, on occasion, can lead to the matter being resolved quickly without recourse to the Courts. As this letter would be sent on your behalf by Eversheds Sutherland, it makes it clear to the recipient that you are taking this matter very seriously. Also, we always recommend in this letter that the recipient should in turn seek independent legal advice as soon as possible.

Dependent on the nature of the unlawful conduct complained of, and the potential damage caused, it is usual in the letter before action to seek further information from the recipient, to request the delivery up of confidential information and equipment, and also to seek the provision of undertakings confirming that they will comply with their obligations going forward. Due to the potential severity of the damage being caused in the interim period, this letter will provide a tight deadline for a response and make clear that if an adequate response is not received then Court proceedings will be issued.

Should the individual (or individuals) have commenced work at another business then we would also recommend writing to this new business to put them on notice of the unlawful behavior and make clear that should they take any steps to induce a breach of contract then proceedings will be brought against them also. This can prove a useful tool in bringing the offender(s) to the table if their new employer had not been previously put on notice of the full position. It also provides another target to make payment of any settlement sums.

In extreme circumstances we may recommend not entering into any pre-action correspondence as in doing so it would put the potential defendants on notice of the fact that their wrongdoing has been uncovered. This could in turn lead to further detriment being caused in the interim period, or crucial evidence being destroyed. Each case is of course different and will be assessed on its merits when we are agreeing a strategy with you.

Court proceedings and applications for injunctive relief

Court proceedings

Should pre-action correspondence be sent and it does not generate a response, or the defendant(s) deny any wrongdoing or fail to provide the information requested, then it may be necessary to prepare and issue Court proceedings. This can be a claim against the ex-employee or director. It also regularly involves a claim against the competitor business that they have moved to on the basis that they have induced a breach of contract, or conspired with the former employee to breach their contractual obligations and/or their common law duties of fidelity and to act in good faith. The remedies sought are likely to include a claim for damages, and will often include the seeking of an order for an account of all business generated as a result of the unlawful behavior. However, in such cases it would be unusual to simply issue a claim for damages without making an application for interim injunctive relief as it is crucial that the wrong doing is equally stopped.

Injunctive relief

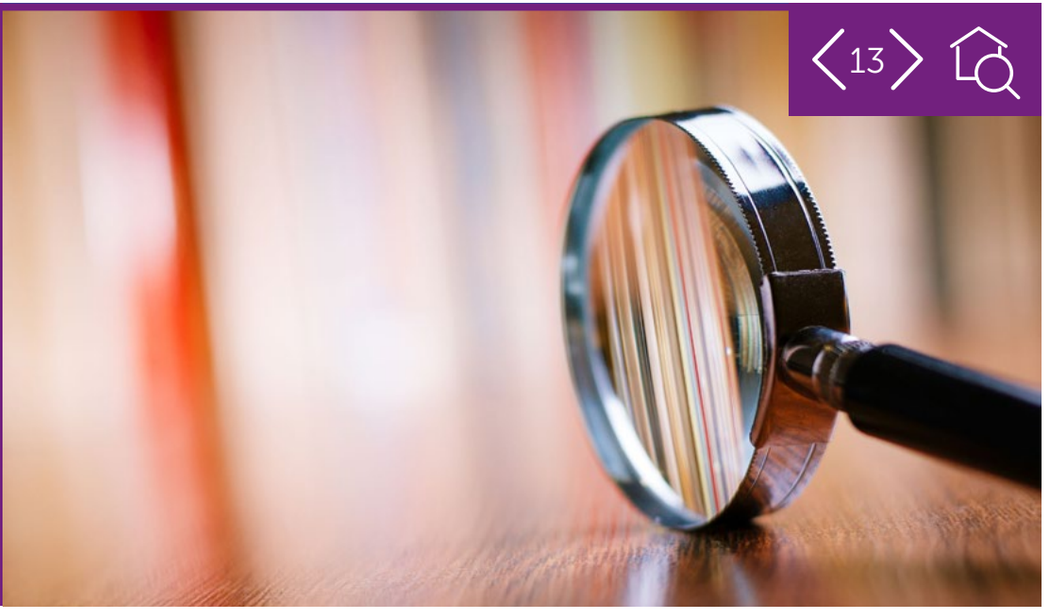
When seeking to enforce post-employment restrictive covenants, common law duties and/or to protect your confidential information, the most appropriate step would be to accompany issuing Court proceedings with an urgent application for an interim injunction order. This order can prohibit the respondent from undertaking certain actions, such as contacting your clients, contacts or staff, for a period pending the outcome of the proceedings. The granting of such an order is an equitable remedy and is at the discretion of the Court. In deciding whether to exercise this discretion the Court will consider the principles set out in the case of *American Cyanamid Co v Ethicon Ltd [1975] AC 396*, which can be summarized as follows:

- whether there is a serious issue to be tried
- whether damages would be an adequate remedy
- where the balance of convenience lies – such as which party would be more prejudiced if the Court were to decide to grant, or not grant, the injunction

When applying for such an order it is imperative that you act promptly. If a party unreasonably delays, an interim injunction may be refused. Equally, if a party goes straight to Court without trying to engage with the other party first, the Court may refuse to grant an interim injunction. However, as explained above, in certain circumstances that may be appropriate and each case must be assessed on its own merits.

It is important to note that the applicant is required to provide a cross-undertaking in damages to the Court that it will compensate the respondent if it is subsequently found at trial that the applicant was not entitled to the relief granted on an interim basis. This must be supported by evidence (normally recent company accounts) that it is able to do so if required.

Options available



Delivery up and search orders

In certain circumstances it is appropriate as part of the injunction application to seek an order for what is known as delivery up i.e. the return of company property. As well as delivery up of documents, an order for delivery up can be made in relation to IT equipment such as laptop computers, memory sticks and mobile phones. Such an order may permit the claimant to take images of the relevant devices in order to retain an "untampered" copy of the systems to be used in the proceedings and to search the devices for relevant evidence. It is possible for our recommended forensic IT colleagues to undertake searches on IT equipment which can identify what activity has taken place, far beyond what the average lay person may be able to find.

Meanwhile a further option available is to apply to the Court for a search order. These orders (often referred to as Anton Piller orders) permit a claimant to search a defendant's premises (which can be either a commercial premises or domestic premises) in order to locate and seize specific classes of documents or other evidence. We utilise this approach in circumstances where there is a significant risk that a defendant will destroy information if they were to become aware of an order for delivery up and, for that reason, such orders applications are made to the Court without notice to the defendant. Given their intrusiveness, search orders are regarded as a draconian power and ordered only in limited circumstances. An independent supervising solicitor is also required to attend to witness the attendance at the premises and ensure that only the steps that are permitted by the order are undertaken.

Springboard injunctions

In addition to the injunctive relief options already discussed, an additional relief available is that which is commonly known as a springboard injunction. This type of injunction is an equitable remedy and its basis is that the Court imposes the injunction to neutralise an unfair advantage that the defendant has obtained unlawfully, such as to prevent it from doing certain things for a prescribed period. For example, it may be used in respect of a defendant who, before leaving their employment, unlawfully took their employer's confidential information relating to clients, and has since been using that information to contact those potential clients until the springboard injunction was granted. These types of injunctions prohibit any further client dealings for a period in order to neutralise the unfair advantage that the defendant had obtained as a result of misusing the confidential information.

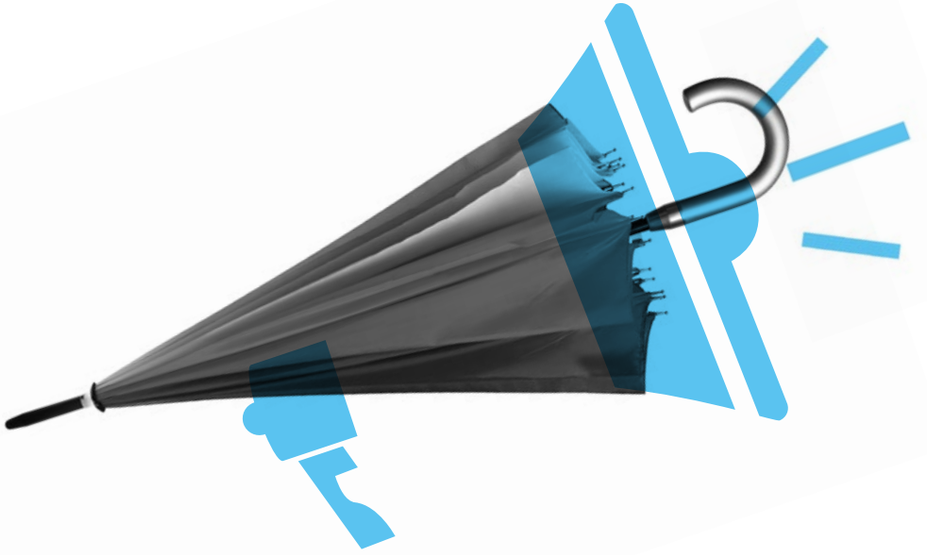
Springboard injunctions can be a useful weapon in team-move situations. The injunction can also provide the basis for imposing a restraint of trade on the defendant irrespective of whether there is any express restraint of trade provision (for example, a non-compete clause, or a non-solicitation/non-deal clause) or if it is questionable whether express provisions can be enforced. Springboard injunctions are most usually (although not exclusively) granted in cases involving a breach of confidentiality. However, applicants have on occasion also been successful in cases regarding senior employees breaching their fiduciary duties and duties of fidelity and to act in good faith.

Any springboard injunction will be granted for a limited period of time only. How long the injunction should last is fact sensitive and should only continue for as long as is necessary to neutralise the unfair advantage which has been obtained. The Court will ensure that the claimant is not given greater protection than it needs, and that the injunction lasts only as long as required to prohibit illegitimate competition.

Settlement

By persuading the Court to grant a form of interim relief, whether that be a prohibitory injunction, a delivery up or search order, and/or a springboard injunction, this provides a very powerful platform in any piece of litigation. The respondents are ordinarily extremely concerned that i) their unlawful behavior has been uncovered and ii) their future in the new role or business is under threat. They are also subject to a Court Order with a penal notice attached to it, which, if breached, can result in severe criminal sanctions.

That being the case, if you succeed with your application on an interim basis it hugely enhances your negotiating position, and in the majority of cases we see settlement negotiations commence very quickly and the dispute is often resolved soon afterwards. These settlement discussions take place in a variety of forms, and can include through correspondence, a Without Prejudice meeting between the parties or, on occasion, a formal mediation. We are extremely dedicated to ensuring that the best possible outcome is achieved for our clients, including the recovery of damages and also the payment of legal costs incurred as part of a settlement.



Data privacy considerations

Employers have a duty to keep personal data secure (whether this pertains to employees or customers). Failure to do so can result in regulatory investigation and/or fines by the Information Commissioner's Office (ICO) and civil claims by the individuals themselves for compensation. Whilst fines are relatively rare in this space, claims by individuals are becoming more common, and perhaps the most significant impact on a business is the damage caused to reputation amongst customers, employees or the public if the data breach becomes widely publicised.

If an employee accesses and retains personal data (e.g. downloading customer lists), in addition to taking action to seek recovery of company property, you will need to consider whether this security breach represents a risk to people's rights and freedoms. If a risk is likely, you need to notify the ICO within 72 hours of becoming aware of the breach. If there is a high risk of individuals' rights and freedoms being adversely affected, the individuals themselves must be informed of the breach without undue delay. You should assess the likelihood and severity of any risk and document your decision.

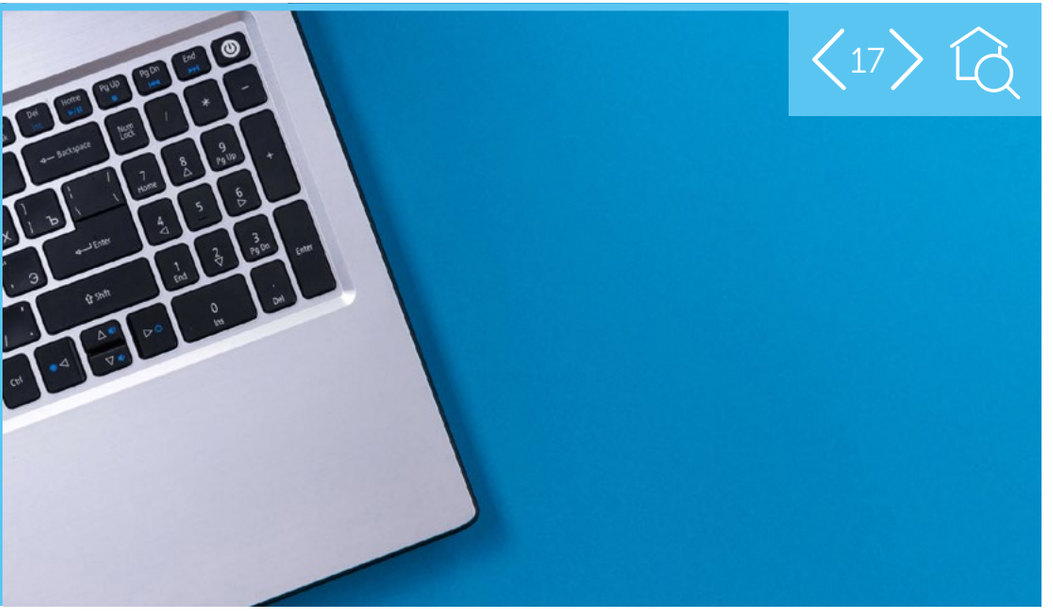
In addition to your duties as a data controller, it is notable that the employee (or former employee) may have committed a criminal offence under the Data Protection Act 2018 and/or the Computer Misuse Act 1990. Highlighting this to the individual could assist your efforts in enforcing your rights for the return of the data. It can also be a significant incentive for the employee to return the data and comply with your requests if their new employer is likely to be informed of the breach.

Whilst the potential impact of a data breach can be significant, if the breach is identified quickly and action is taken to recover and secure the data without delay (in any event within 72 hours of discovery), it may be possible to avoid the need to notify the ICO or individuals. We have a team of employment, privacy and litigation lawyers who regularly work together to manage such situations. Seeking immediate advice is key to managing the risks in this regard.

Our legal bit:

This guide is intended to give an overview of the main legal tools available, to assist with the protection of your business. It does not set out a comprehensive picture of the law in all of the areas covered and is not tailored to any particular circumstances your company may be facing. It should not therefore be seen as a substitute for carrying out research or obtaining legal advice, both of which we would be very happy to assist with.

Contact details



Should you wish to discuss any of the issues raised in this guide, arrange a review of the protection that you currently have in place, or obtain our support on a matter involving an ex-employee or team, please do not hesitate to contact us

Phil Duignan
Partner

T: +44 161 831 8509
M: +44 739 325 4381
philduignan@
eversheds-sutherland.com

Jenny Mann
Principal Associate – Employment, Labor and Pensions Group

T: +44 161 831 8134
M: +44 790 989 0143
jennymann@
eversheds-sutherland.com

Dave Hughes
Partner

T: +44 122 344 3642
M: +44 782 793 6225
davidlhughes@
eversheds-sutherland.com

eversheds-sutherland.com

DTUK002960_07/21