# People and confidential information: Dealing with key employment risks

AIMA SPONSORING PARTNER

MACFARLANES

*By Hayley Robinson, Partner, Macfarlanes and Matthew Ramsey, Professional Support Lawyer, Macfarlanes*

Amongst a firm's key assets are its people and its proprietary information. This article looks at some of the risks affecting these two areas, and discusses strategies to ensure firms are adequately protected. In particular, we'll look at how to ensure confidential information is properly protected, and what steps are available to restrict key people moving to competitors.

## Confidential information

Firms naturally regard their proprietary information as critical to their success in the market – but people are leaky and IT systems are not fool-proof. The explosion of mobile devices and wearables in recent times poses an increased risk of confidential information leakage. Many financial services clients prohibit smartphones in the front office, for sound risk management and regulatory reasons. But what other steps can and should firms be taking to lock down business-critical information, whether that is investor lists, trading algorithms or employee data?

The answer usually comes in three parts: have a clear policy setting out what is acceptable; have an effective means of enforcing that policy; and have enforceable restrictions to operate during notice periods and post-termination.

## Policies

The common law gives an employer relatively little protection in relation to confidential information, generally only restricting the disclosure or use of trade secrets. Trading algorithms might fall within that category, but in order to protect other forms of information an employer will need clear contractual provisions coupled with a clear policy. These ought to describe in granular detail the types of information that are regarded as confidential and restricted, and should give employees clear guidance on what they may and may not do.

## Monitoring and enforcement

Although setting clear rules is a necessary first step, in the modern age the real challenge lies in the policing. Employees are seldom foolish or naïve enough to use work email to prepare for their departures, so firms need to address all the myriad ways in which data can be disseminated. Instant messaging systems, smartphones and social media platforms all offer opportunities for unscrupulous employees, particularly in firms which operate BYOD, or 'bring your own device' arrangements. This is an increasingly popular means of reducing IT budgets, and sees proprietary software loaded onto an employee's own device (tablet or laptop etc) so the employee can efficiently work remotely.

As emails and messages continue to be routed through the employer's systems in a BYOD arrangement, firms should continue to be able to monitor usage as if the employee were at their desk. The European Court of Human Rights analysed in January what types of monitoring of behaviour are permissible, and the decision largely mirrors what is established best practice in the UK.

The court's judgment in Bărbelescu v Romania [2016] ECHR 61 was widely reported in the press as giving a green light to all forms of monitoring. In reality, the position is rather more nuanced and the case was heavily influenced by the particular facts. In brief, Mr Bărbelescu set up a Yahoo! Messenger account for work purposes and was very clearly told that no private usage was permitted. He used the account for private discussions notwithstanding that instruction, argued when challenged that he had never used it for personal matters, and then sought to argue that his employer should not have monitored the account to prove he had in fact done so.

Unsurprisingly, given those facts, the Court found Romanian law permitting the monitoring to be compliant with the over-arching human right to respect

continued ▶

for private life and correspondence. But that is not the same as ruling in favour of unrestricted monitoring. In the UK, legislation and, in particular, the Information Commissioner's Employment Practices Code make clear that monitoring will usually be permissible if:

- The employer carries out a risk assessment before embarking on monitoring
- Employees are informed in advance (usually via the employer's policies) that monitoring may be carried out, what will be monitored, why, and what will be done with the results
- The employer acts in a reasonable and proportionate way: this covers every aspect of data processing and collection, from choosing the least intrusive method of monitoring, to considering how long the results will be retained and who will have access to them

If the confidential information provisions are well drafted, the IT and disciplinary rules are clear and the monitoring system is effective, firms should be able to feel safe in taking a robust line.

## Notice periods, garden leave and post-termination restrictions

Inevitably, misuse of confidential information usually takes place when an employee is contemplating a move and there are additional methods of protecting business-critical information at that stage.

Well-drafted employment agreements will typically allow the firm to send an employee home for part or all of their notice period – garden leave. Garden leave provisions will usually restrict the employee's contact with investors, other employees and clients, and contractual restrictions on the use of social media are now increasingly common.

Some firms use lengthy notice periods, often by agreeing to fixed-term contracts without a break clause or other notice provision. Even though employees continue to draw salary and benefits during notice, they are often reluctant to spend lengthy periods out of the market, and the courts will generally only force an employee to sit on their hands for a limited period.

Fixed-term contracts and long notice periods are also common methods of tying employees into a firm. Often coupled with closely-limited notice windows, they can be effective ways of blocking an employee from going elsewhere. But inevitably some employees will leave and try to evade garden leave-type arrangements. For that reason it's important to have in place restrictions that operate post-termination. Restrictive covenants preventing an ex-employee from working for a competitor or soliciting clients or investors can be enforceable, but only if they go no further than is reasonable to prevent a firm's legitimate business interests. Those interests can include the protection of its confidential information, the stability of its workforce, and the maintenance of its client or investor relationships. Post-termination restrictions are often viewed as difficult to enforce, but there are numerous examples of the courts enforcing lengthy restrictions, particularly in the financial services sector. It would be a mistake to disregard them when developing a suite of strategies to protect key information or employees.

Firms may be able to achieve a higher degree of protection in relation to their LLP members, including by making use of the court's traditional willingness to permit longer restrictions against partners and other business owners. Some fund documentation also seeks to prolong a partner/member's period of restraint by using the (largely untested) tactic of indirect restraints often linked to a period of passive membership where the partner ceases to have any role in the firm, but continues to have an economic interest in one or more funds.

Firms cannot operate without good people and good information. Keeping the information flowing but secure, and keeping both people and information from competitors for as long as possible are key aims that, with care, do not need to be mutually exclusive or unattainable. The challenges posed by technological development and social media means that the law is often behind the curve, but as demonstrated in this article, there remain a number of sensible preventative precautionary steps firms should take to protect their positions.

hayley.robinson@macfarlanes.com
matthew.ramsey@macfarlanes.com
www.macfarlanes.com