Consequences of an employee sharing company secrets with competitors

Employees have a duty of confidentiality and good faith to their employers and employers have a right to ensure that company information is not misused or wrongfully disclosed. But what happens when a company's information is 'stolen' and ends up in the hands of a competitor?

The unauthorised disclosure of confidential information or sharing of company secrets constitutes a breach of the employee's duty of confidentiality and can have important consequences. This was evident in recent proceedings before the Federal Court of Australia - *Show Pony Group Pty Ltd (Showpo) v Black Swallow Boutique & Ors (Black Swallow)* (File No. NSD1984/2016).

The case flags important issues for employers - the security risks associated with the use and management of online data and the fact that a breach of confidence often occurs internally.

Case study

Showpo and Black Swallow are on-line fashion retailers with similar target markets.

Showpo alleged that a former employee downloaded information containing some 306,000 contacts shortly prior to resignation, for the benefit of her new employer Black Swallow. The database contained significant information including a customer mailing list, subscribers and competition entrants and contacts of suppliers.

When Showpo learned that Black Swallow had started using the database for its next marketing campaign, proceedings were filed in the Federal Court.

The first stage of proceedings was for Showpo to seek an urgent interim injunction, which is a Court order immediately preventing Black Swallow from using the information for a specified period or until proceedings are finalised. This was an integral step to control the foreseeable damage that Showpo might suffer from unauthorised use of its database.

The case was ultimately settled through assisted mediation. By consent, the Court ordered that the respondents (Black Swallow, its chief executive and Showpo's ex-employee) be permanently restrained from using or disclosing the client contact list or

any information derived from it and that they pay Showpo $60,000 as compensation. Each party was required to meet its own legal costs.

Take home messages for businesses

Business rivals are anxious about guarding trade secrets and confidential documents from exploitation. There are various steps employers can take to help protect against unauthorised disclosure.

On-line security management

Employers should evaluate and monitor their IT systems, policies and procedures. It is important to set very specific rules when determining who has access to confidential information and how that information may be used.

To minimise on-line security risks, a business can take the following steps:

- Work with an IT professional to ensure that they understand their computer systems and that all possible security, storage and backup devices are available and being used effectively.
- Ensure that access to confidential or sensitive information is provided only as absolutely necessary and that records are kept with details of those employees who are granted access.
- Educate staff about on-line security safety and scams or unauthorised access attempts and require that any suspicious activity be immediately reported.
- Reiterate the importance of creating strong passwords and keeping them confidential. Passwords should avoid birth dates, street names, family or pet names, etc., and be updated regularly. Passwords should never be shared with other staff members and a one-password-fits-all approach is a recipe for disaster.
- Ensure that an outgoing employee's access to information is immediately terminated upon his or her departure and passwords reset. Depending on the circumstances, employers might also consider whether access should be suspended before the last day.
- Use employment agreements, policies and codes of conduct to document employee expectations regarding IT security and computer use.

Employment agreements

Although a duty of confidentiality is implicit within the employment relationship, employers should use written contracts to reiterate the employee's obligations.

Incidental workplace matters and employee expectations regarding computer use and confidentiality should also be spelt out in company policies and codes of conduct which should be made available to all employees before or on induction.

Confidentiality and trade secrets can be further protected through restraint of trade clauses in the employment contract.

The intention of a restraint of trade clause is to prevent an employee after leaving the workplace, from using confidential information and / or working with certain competitors within a certain area and or for a specific time. Restraint of trade clauses must be carefully drafted to ensure they are reasonable and only go so far as to protect the legitimate interests of the business. Restraint clauses that are too onerous or too broad risk being struck out by the Court.

Seek legal advice

It is important to act quickly if you believe an existing or former employee has misused confidential information. In many circumstances, the Court will grant an urgent injunction restraining the recipient of the confidential information from using the data until proceedings are finalised.

Further legal remedies include permanent injunctions, awards to compensate the innocent party for any loss suffered from breach of contract, damages for infringement of copyright and costs orders.

If you are aware that an existing employee is breaching confidentiality it is important to obtain advice on how to address the conduct and, if necessary, lawfully terminate the employee.

Conclusion

The sharing of a business's confidential information often comes from within its own walls - when a disgruntled employee or opportunist leaves one company to go to another which is very-often a participant in the same market.

An experienced lawyer can assist in preparing effective employment agreements containing confidentiality and restraint clauses and provide guidance on developing policies addressing on-line security risks.

If you or someone you know wants more information or needs help or advice, please contact us on (03) 9600 0162 or email info@lordlaw.com.au.