Intellectual property protection for trade secrets and know-how

Thomas Duston and Thomas Ross
Marshall, Gerstein & Borun, Chicago, IL

A trade secret is virtually anything that is secret, and that imparts value to its holder as a consequence of that very secrecy. Technical and scientific information, such as formulae, manufacturing methods and specifications, designs, computer code and the like receive protection as trade secrets. Commercial and financial information may also qualify as a trade secret. Customer lists, customer buying preferences and requirements, the identity of customer decision-makers, pricing information, marketing and business plans, internal cost structure, supplier arrangements, and other similar non-public information can be protected.

Even so-called ‘negative’ information may receive protection as a trade secret. For example, the details of failed efforts to remedy problems in the formulation or manufacture of certain products, dead-ends encountered in research, abandoned technical solutions, or the unsuccessful attempts to consummate sales or interest various customers in purchasing a company's product or service, may each receive protection as a trade secret. Such ‘negative’ information has value to a competitor as a guide to what not to do, potentially providing a competitor with a no-cost head-start.

Unlike patented technology, a trade secret need not be novel. In fact, a trade secret, such as a customer list, may represent nothing more than a compilation of otherwise publicly available information. If the overall compilation is not readily ascertainable by competitors, the fact that individual components of the overall compilation of information could be obtained from publicly available sources does not preclude protection.

Patent or copyright protection generally requires one to make some disclosure or publication of the information. Temporary protection is then afforded for a period of years, after which the information becomes freely available to the public. Trade secret protection exists for as long as the holder is successful in maintaining the secrecy of the information. If commercial exploitation of the information necessarily results in its disclosure, such as where a product itself reveals the information, then patent or copyright protection is more appropriate. Where it is possible to keep the information from prying eyes, such as with an internal manufacturing method or formula, trade secret protection is preferred. Indeed, in such circumstances, patent protection may be less effective due to the difficulty in identifying infringements.

Trade secret laws, however, do not grant the holder the exclusive right to exploit the secret information. Others may develop the information independently. They may even derive it by reverse engineering the trade secret owner’s product.

Law governing trade secrets

Until relatively recently, trade secret protection was the exclusive province of state law. In 1996, Congress passed legislation making it a federal crime to misappropriate trade

secret information, with heightened penalties if the misappropriation was intended to benefit a foreign entity. Despite the existence of this relatively new federal law, and similar criminal statutes passed in various states, the vast majority of trade secret enforcement occurs through civil suits brought by the holder against the alleged misappropriators under state law.

By 2001, 43 states and the District of Columbia had passed laws patterned on the Uniform Trade Secrets Act. The exceptions are Massachusetts, New Jersey, New York, North Carolina, Pennsylvania, Texas and Wyoming. This Act is the result of the efforts of the National Conference of Commissioners on Uniform Laws to standardise statutes relating to this and other topics around the country. In those states that have not passed statutes protecting trade secrets, protection is afforded under the state's common law.

Under the Uniform Act, a trade secret is defined as ‘information that derives independent economic value, actual or potential, from not being generally known to, and not being readily ascertainable by proper means by, other persons who can obtain economic value from its disclosure or use.’ To qualify as a trade secret, the information must also be ‘the subject of efforts that are reasonable under the circumstances to maintain its secrecy.’

Under the Act, a trade secret is ‘misappropriated’ when it is acquired through improper means, or where it is disclosed or used without the express or implied consent of the trade secret owner after having been acquired under circumstances giving rise to a duty to maintain its secrecy. ‘Improper means’ include theft, bribery, misrepresentation, breach or inducement of a breach of a duty to maintain secrecy, or espionage through electronic or other means. Misappropriation under the Uniform Act may also occur where a party uses or discloses information it acquired by accident or mistake, provided that party had notice that the information constituted the trade secret of another before that party materially changed its position based upon its belief that the information was unprotected.

In those states which have not adopted some variation of the Uniform Act, courts are generally guided by the Restatement (First) of Torts. Published first in 1939, the Restatement represented an effort to summarise the then-existing state of the law. Under the Restatement, whether information is a trade secret depends upon:

1. the extent to which the information is known outside the holder's business;
2. the extent to which it is known by employees and others within the business;
3. the extent of the measures taken to guard the secrecy of the information;
4. the value of the information to the holder and its competitors;
5. the amount of effort or money expended in developing the information; and
6. the ease or difficulty with which the information could be properly acquired or duplicated by others.

The Restatement approach differs in significant respects from the Uniform Act. Among those differences, the Restatement requires the information to be in ‘continuous use’ by a business, raising questions concerning the protection of negative information in those

jurisdictions strictly adhering to its formulation. The Restatement also affords a safe harbour, unavailable under the Uniform Act, to innocent acquirers who purchased the information for value in good faith, or who otherwise materially changed their positions, without knowledge of its trade secret character. Under the Uniform Act, a safe harbour is available only where disclosure of the trade secret has occurred by mistake or accident, and not as a result of any improper actions of another, such as theft by a former employee. The party receiving the information, however, must still have materially changed its position before receiving notice that the information is a trade secret. More recently, the Restatement (Third) of Unfair Competition has updated the earlier Restatement's treatment and is more in line with the Uniform Trade Secrets Act. This treatment is gaining acceptance among courts in those states that previously adhered to the earlier Restatement's formula.

In addition to an action under the Uniform Trade Secrets Act, a trade secret owner may have available other remedies for breaches of contract or of existing fiduciary duties of loyalty owed by employees or officers. If a third-party, such as a new employer, is involved in the alleged misappropriation, allegations that it has tortiously interfered with the holder's rights may also exist. Other causes of action that focus more on the means by which the information is acquired or removed, rather than the information itself, may also be available. For example, misappropriation may have entailed unauthorised access to computer systems in violation of statutes governing computer trespass, such as the Federal Computer Fraud and Abuse Act. If misappropriation involved the physical removal of documents or records, an action for return of the property might impede continued or additional use or dissemination and require less rigorous proof.

Required security precautions

The existence of reasonable security precautions is an essential element of a protectible trade secret. Security precautions have several purposes. They provide evidence that the information has remained secret. Investment in such precautions demonstrates that the information has value to the holder. Their existence provides notice to employees and others that the information is confidential, and that its unauthorised use or disclosure will be considered improper.

Courts have deemed a number of precautions adequate. Generally, a trade secret owner should employ as many of these procedures as it reasonably can in order to enhance protection of its information. These procedures include: restricting access to the information physically and electronically to only those individuals having a need to know of the information; marking documents or their storage areas with notices that the information is deemed proprietary and confidential; notices contained in employee handbook; the use of non-disclosure or confidentiality agreements with those granted access; maintaining the information under lock and key or imposing password protections on access to the information; monitoring access to the information through log-in procedures, sign-in sheets and the like; disposing of the information by shredding or other means designed to eradicate the information; exit interviews for departing employees to ensure return of all confidential information and to emphasise confidentiality obligations; and, the aggressive pursuit of instances of alleged misappropriation, among others.

These procedures need not result in absolute secrecy for the information. What constitute reasonable precautions depends on the circumstances. In a case involving DuPont's method for producing methanol, for example, the misappropriator acquired the information through aerial photography of DuPont's facility during its construction. The court found that it would be unreasonable to require that DuPont build a roof over its unfinished plant as a precondition to protecting its trade secret method.

Use of non-competition agreements

Confidentiality agreements and other security precautions may, however, prove inadequate to protect against improper use or disclosure of a trade secret. Employees and suppliers, for example, often gain extensive and continuous exposure to this information. Trade secret information, particularly negative information and that concerning future strategies or plans, may influence a competitor in subtle ways, difficult to evidence. A non-competition agreement that imposes bright-line limits on the subsequent activities of the employee or supplier is often used to minimise the opportunity to use or disclose the trade secret.

Courts carefully scrutinise such agreements. Such agreements must not only be directed to the protection of a legitimate business interest, such as a trade secret, but they must also be no more restrictive than is reasonably necessary for the protection of that interest. An employee always remains entitled to use his general knowledge, skills and experience gained during his employment to later compete with his former employer.

The non-competition agreement must tailor its restrictions to the actual information shared with the employee or supplier. The non-competition agreement must also limit the restraint to an appropriate geographic area. It must expire after a relevant period of time, ordinarily measured by the time necessary for a competitor to develop the information independently.

Even in the absence of a non-competition agreement, courts will sometimes fashion the equivalent where use or disclosure of the trade secret is inevitable. Where, for example, an employee takes a position with a competitor in which he or she cannot avoid using or disclosing the information, a court may determine that the only way to ensure compliance with the employee's non-disclosure obligations is to prohibit the employee from accepting the employment. This is known as the 'inevitable disclosure doctrine'.

Enforcement of trade secret protection

To redress the violation of trade secret rights, the available remedies are damages, injunctive relief, accounting for profits, and destruction of wrongfully made goods, patterns, and the like.

Courts will allow the recovery of the trade secret owner's losses, and any additional unjust enrichment enjoyed by the misappropriator. Where the misappropriation is deemed willful and malicious, the Uniform Trade Secrets Act permits the enhancement of damages of up to twice the award of actual damages or profits, and the recovery of

attorneys' fees. The decision as to how much should be awarded is left to the discretion of the judge.

Several types of injunctions are available in trade secret cases. Due to the imminent risk of loss of the trade secret, temporary injunctive relief, sometimes referred to as a temporary restraining order, is usually sought immediately upon commencement of the lawsuit. A temporary restraining order is limited in duration, generally in force until a hearing can be held on a request for a preliminary injunction. The purpose of a preliminary injunction is to preserve the status quo until the case can be tried, preventing further use or disclosure of the trade secret while the case is pending. Obtaining a preliminary injunction usually requires a hearing involving the presentation of evidence and witness testimony, much like a trial. A final injunction prohibiting the use or disclosure of the trade secret may then issue following trial. The enjoined party, however, remains able to seek termination of the final injunction when the trade secret becomes generally known through legitimate means. It is possible and sometimes strategically better for the trade secret owner to consolidate the preliminary injunction hearing with the trial on the liability case, with the issues of damages and punitive remedies being postponed for a separate trial. In circumstances where the court deems injunctive relief inappropriate, it may choose to direct that the misappropriator pay an ongoing royalty.

The trade secret owner is often faced with a Catch-22: to establish a violation of its trade secrets, it must disclose that secret during litigation. Typically, however, a protective order is issued early in a trade secret case upon motion to the court which limits dissemination of the identified trade secret information to outside counsel for the parties, independent experts, and perhaps a few, necessary employees of the parties and restricts use of the trade secret information only for purposes of the lawsuit. The protective order provides for the return or destruction of the identified trade secret information upon conclusion of the lawsuit.

Licensing of trade secrets

The trade secret owner may grant exclusive, sole, or non-exclusive licences. The license may be limited to certain territories, customers, or product markets, and otherwise permit the licensor to continue to practice the trade secret along with the licensee in those areas not exclusive to the licensee. There may also be cross-licence agreements in which the parties exchange trade secrets.

Payment by the licensee for use of the trade secret may take various forms. If it is a royalty, the royalty may be based on such criteria as manufacturing throughput, product sales price, cost savings, or increased or gross sales. Of course, the trade secret licence typically restricts the disclosure of the trade secret. Once the trade secret ceases to be a secret, the subject matter of the licence will have disappeared. Disputes may arise regarding whether the licensee must continue to pay royalties under a licence where the trade secret has become known. Parties may wish to address this contingency, establishing rules where disclosure was the fault of one, or the other, or neither party.