

NON-DISCLOSURE AGREEMENTS PROTECT COMPETITIVE EDGE

By David E. Dubberly

Employers must take proactive steps to make sure that their trade secrets are protected to the fullest extent permitted by South Carolina and federal law. One step to prevent theft of confidential information by competitors and/or employees is to require employees to sign covenants not to disclose trade secrets during or after employment. Non-disclosure agreements are often combined with policy statements, exit interviews, and acknowledgement forms for departing employees. An overview of the legal protections available for trade secrets and the issues involved in using non-disclosure agreements follows.

Legal Protection of Trade Secrets

Common Law Protections. South Carolina courts protect an employer's trade secrets from "misappropriation." A trade secret may include any information not generally known to or readily ascertainable by competitors, such as information about customers, prices, production methods, and marketing plans, as long as the employer takes steps to guard the information's secrecy. Requiring employees who have access to trade secrets to sign non-disclosure agreements is one important step that employers can take to guard the secrecy of the information.

Under the judicially-created common law, an employee "misappropriates" trade secrets if the employee understands that the information was shared with him in confidence, but he nevertheless makes an unauthorized disclosure of the information, usually to his new employer.

Statutory Protections. The South Carolina Trade Secrets Act (SCTSA) makes it unlawful for an employee to disclose his employer's trade secrets. The federal Economic Espionage Act (EEA) makes it a crime to take, copy, or receive trade secrets without the permission of the owner of the trade secrets. These laws provide protection even if an employee never signed a non-disclosure agreement.

Remedies. In South Carolina, employers whose trade secrets have been misappropriated may file suit requesting:

1. a preliminary and/or permanent injunction against disclosure;
2. damages for any actual losses suffered by the employer and any amounts that the person misappropriating the trade secrets may have unjustly received; and
3. "exemplary" (double) damages if the offending employee acted in a "willful, wanton, or reckless" manner, plus attorney's fees if the employee acted in bad faith.

In addition, the SCTSA and EEA create criminal penalties for trade secret theft. Penalties include a maximum fine of \$5,000,000 and a maximum prison sentence of 10 years.

Recommendations for Employers

Employers should take the following additional steps to enhance the secrecy and security of confidential information, and to strengthen their position in potential legal battles.

1. Require employees with access to trade secrets to sign non-disclosure agreements. Consider including the following clauses in the agreements:

- (a) Forum selection, choice of venue, and choice of law clauses to give the employer a “home court” advantage in the event of litigation. (Be aware that courts will not always enforce forum selection clauses against some non-resident employees.)
- (b) A provision permitting the employer to assign the agreement without the employee’s consent to any successor, joint venture partner, or corporate parent, affiliate, or subsidiary of the employer.
- (c) A clause requiring the employee to inform his subsequent employers about the agreement.
- (d) A “Tattle-tale” provision, requiring the employee to report to the employer all unauthorized disclosures or uses of the employer’s trade secrets or confidential information that come to the employee’s attention.
- (e) A clause providing that if the employee has a question about whether specific information is considered confidential, he or she must request a written clarification from a designated company official.

2. Include a policy statement regarding confidential information in the employee handbook as an additional layer of protection. A signed acknowledgement form stating that the employee received, read, and understood the handbook should be kept in each employee’s personnel file. Employers also should have a policy for protection, retention, and destruction of confidential documents, including procedures for marking confidential documents with a statement such as “Confidential-Proprietary Information of [name of employer].”

3. Conduct exit interviews with departing employees. An exit interview gives the employer the opportunity to review with the employee the terms of the non-disclosure agreement (as well as any non-compete and non-solicitation agreements) and to emphasize the employee’s obligations. The meeting will also remind the departing employee that the employer is prepared to enforce the agreement and that the employee cannot remove any confidential

information from the employer's premises. The exit interview also may alert the employer that the employee is about to engage in activities that violate the agreement, and that a close monitoring of the employee's activities is warranted. During the exit interview, present the employee with an exit acknowledgement form. The form should ask the employee to provide the following information:

- (a) the name of the new employer, the employee's new work and home addresses, the commencement date of new employment, and the employee's responsibilities and duties in the new employment;
- (b) an acknowledgement or reaffirmation of the employee's obligations regarding confidential information; and
- (c) an acknowledgement that the employee has returned all originals and copies of all confidential documents and information to the company.

4. Additional examples of security measures employers can use to prevent the disclosure of confidential information include:

- (a) storing confidential information in locked files and locked rooms;
- (b) limiting employee access to confidential information on a need-to-know basis;
- (c) using pass codes for computer access and changing the codes on a periodic basis;
- (d) limiting computer access for certain types of information; and
- (e) restricting visitor access to areas in which secret processes or machines operate or are being developed, and requiring all visitors to sign a log stating the visitor's name, address, telephone number, purpose of visit, etc. All visitors should be escorted by appropriate employees.

5. Act swiftly and decisively when the integrity of confidential information is threatened. This may include sending a cease-and-desist letter to any former employee who breaches his non-disclosure agreement (and possibly the new employer), initiating criminal proceedings, or filing a civil lawsuit.

In conclusion, trade secrets are assets that have monetary value and must be protected by taking affirmative steps. The more important and confidential the information, the more stringent the measures an employer should take to protect the information.