FRIEND, HUDAK & HARRIS, LLP
ATTORNEYS AT LAW
Three Ravinia Drive, Suite 1450
Atlanta, Georgia 30346-2117
(770) 399-9500
FAX (770) 395-0000

BRIEFING ON INFORMATION TECHNOLOGY LAW

by Mari L. Myer, Esq.[1]

The Georgia Trade Secrets Act and Inevitable Disclosure

I. Introduction to The Georgia Trade Secrets Act

Georgia, like many states, has enacted a Trade Secrets Act prohibiting the misappropriation of information which, regardless of the form in which it is maintained, satisfies the definition of a trade secret. Typically the application of the Trade Secrets Act is triggered when an employee[2] leaves one employer to work for another one. At that point, concern may arise over whether the employee will (either consciously or unconsciously) use or disclose to the new employer trade secrets belonging to the first

[1]Ms. Myer is an attorney with the firm of Friend, Hudak & Harris, LLP in Atlanta, Georgia. A graduate of Wellesley College, *cum laude*, and Boston University School of Law, Ms. Myer has a business litigation practice with a focus on issues involving trade secrets, restrictive covenants and technology matters.

[2]For purposes of this article, the term "employee" refers to both employees and independent contractors.

employer.[3] This article addresses the basics of the Georgia Trade Secrets Act, as well as recent developments in the arena of "inevitable disclosure" - the doctrine that in some circumstances an employee cannot be allowed to work for a competitor in certain capacities because such employment will inevitably cause the employee to disclose trade secrets belonging to the first employer.

II. What is Protected as a Trade Secret

The Georgia Trade Secrets Act, O.C.G.A. §§10-1-760 *et seq.,* provides protection for information which, without regard to its form, (a) is the subject of efforts to maintain its secrecy and (b) derives its value from the fact that it is not generally known to the public. Trade secrets may be protected indefinitely, so long as they continue to comply with the aforesaid criteria. Examples of trade secrets include computer software, written customer lists, written supplier lists, formulae, compilations, programs, financial data, and product plans.

---

[3]In some instances, the employer may also have available protections under copyright law. Such protections are beyond the scope of this article.

An employee's skill or general knowledge developed in the course of employment is not subject to trade secret protection.[4] A good rule of thumb is that general information about the employer is probably not subject to trade secret protection; but that the more specific the information is, and the more critical it is to the employer's success, the more likely it is to be regarded as a trade secret so long as it is the subject of appropriate efforts to protect its secrecy.

III. Protecting Trade Secrets From Disclosure

The information which the employer seeks to protect as a trade secret must be kept secure. For example, information which is kept on a computer should be protected by passwords, with passwords changing frequently. When an employee with password access terminates employment, his password should be deactivated. It is not wise to assign the same password to several employees: if one of these employees were to leave, all employees with this password should be assigned a new password.

It is also useful to obtain signed nondisclosure agreements from persons with access to the trade secrets, thereby documenting that these persons have been placed on notice that trade secrets exist and must be kept confidential. Trade secrets should be described to employees (preferably in writing) with sufficient specificity to enable the employees to determine the types of information which they are required to keep confidential. Trade secrets should also be kept under lock and key, and their disclosure restricted to employees with a "need to know". Some employers find it useful to remind employees of the nature of their obligations with respect to trade secrets during staff meetings and in company memoranda and emails. When the very core of the employer's business is at stake, even stronger protections may be called for.

The reasons for these protections are twofold: first, since the employer's goal is to prevent the disclosure of the trade secrets, the employer should make it as difficult as possible for such disclosure to occur; second, in the event that the information is nevertheless disclosed, it will be essential to be able to demonstrate to a judge and jury adequate efforts to protect the information so as to satisfy the "efforts to maintain secrecy" prong of the definition of "trade secret". Absent evidence of adequate efforts to protect the information, not only will the information be lost but the owner of the information will not be allowed to employ the remedies available under the Georgia Trade Secrets Act.

---

[4]Information which is important to the business but which does not rise to the level of a trade secret can often be protected in a nondisclosure covenant. These covenants were the subject of a previous Memorandum to Clients and Friends.

IV. The Doctrine of Inevitable Disclosure

Although the Trade Secrets Act states that information which otherwise meets the definition of trade secret will be protected without regard to its form, in general Georgia courts have only protected as a trade secret information which is somehow permanently stored (*e.g.*, a writing, a computer program, a blueprint). But the Georgia Supreme Court has recently applied the doctrine of "inevitable disclosure" to prevent an individual from developing for a competitor from his memory a trade secret logistics system like the one he had developed for his previous employer. Even though there was no evidence that this individual had taken any written materials or computer files with him regarding the development of the logistics system, the evidence established that this person was capable of reconstructing from memory significant portions of the logistics system. Because he had helped create the system in the first place, he likely would be able to create a similar system for his second employer, and almost certainly would be able to do so more efficiently than the first time around. The system was complex and had resulted in significant financial benefit to the first employer; thus the development of a similar system by this former employee for a competitor would have resulted in financial benefit to the competitor and a diminution in the value of the benefit to the first employer. Under these circumstances, the court barred the employee from working for the competitor in the capacity in which he had worked for the first employer.

This situation may be contrasted with reverse engineering, in which a competitor may attempt to determine how to develop a product by taking it apart. This is countenanced in the Georgia Trade Secrets Act, so long as the person engaged in this reverse engineering did not acquire the trade secret by misappropriation. To protect against a misappropriation claim when engaged in reverse engineering, a business should avoid assigning to the project personnel who previously worked on the development of the product which is the subject of the reverse engineering.

To date, Georgia appellate courts have only applied the doctrine of "inevitable disclosure" in one case. The doctrine has been applied on a few occasions in other jurisdictions. But some states appear to be backing away from this doctrine. Therefore, it is difficult to predict whether this doctrine will be applied in any given situation. But in those situations in which it is applied, the result can be that the employee in question will be precluded from accepting employment with a direct competitor of his previous employer, and any product on which the employee worked for the competitor may be deemed to be tainted with trade secrets belonging to the first employer. Therefore, it is crucial that concerns about possible application of this doctrine be addressed at the time of hiring so as to minimize the exposure of the employee and subsequent employers to application of the inevitable disclosure doctrine.

V. Protections In the Event of Misappropriation of Trade Secrets

In the event that a trade secret is disclosed or used without the employer's authorization - "misappropriated" - the employer will be entitled to an injunction to prevent further misappropriation of the trade secret. Indeed, injunctive relief may in some instances be had even if the misappropriation is merely

threatened, so long as the court is satisfied that such misappropriation is imminent. The injunction may be issued against any person or entity which has obtained unauthorized access to the trade secret. In the context of software development, the result may be that further development of software deemed to be derived from misappropriated trade secrets will be enjoined, or a royalty may be assessed on the revenue from the sale of the software. Where a royalty cannot be calculated, compensatory damages equivalent to the trade secret owner's losses from the misappropriation may be awarded instead. In addition, attorney's fees and exemplary damages representing double the royalty or double the compensatory damages may be awarded.

About the Firm

FRIEND, HUDAK & HARRIS, LLP concentrates its practice in the representation of information technology clients. The Firm's attorneys combine extensive experience in corporate/ commercial law with mastery of computer/communications law and intellectual property. As a result, the Firm is uniquely suited to represent growing information technology companies across all areas of corporate, commercial and information technology law.

These materials are merely a summary, published for tutorial purposes only, and are not published for the purpose of rendering legal advice.