

Article

The Law of Trade Secrecy and Covenants Not to Compete in Colorado—Part I

by John F. Reha

In the past ten years, few areas of the law have experienced the exponential growth as those of trade secrecy and competition restrictions. The advent of technology and the coming of age of the "dot.com" world have only accelerated a process of legal development, which was already in a state of rapid growth. In the post-industrial, information-based economy, increasingly it is information that is the key asset of business. In the industrial age, hard assets were the lifeblood of most businesses, but they have now been relegated to the supporting role of tools. Many businesses sell information, others market concepts, and still others sell identity. Thus, fewer new businesses are involved in the sale of tangible items, at least in the traditional, "bricks and mortar" sense.

Moreover, for all businesses, even those involved in traditional inventory-based industries, knowledge and relationships are increasingly proving to be the core value of organizations. Sales personnel with a large network of contacts and designers and engineers possessing "know how" commonly hold in their hands the key to the value of the entire enterprise (or at least a critical part of it). The law has attempted to keep up with these fundamental changes. That attempt is often through the concepts of trade secrecy and covenants not to compete. This article addresses a number of those developments, with an emphasis on the law of Colorado.

The first part of this two-part article focuses on trade secrets. The second part, to be published in the May 2001 issue, will discuss covenants not to compete. These articles have two purposes: (1) to afford Colorado practitioners a greater understanding of the substantive law in the areas of intangible asset misappropriation and competition; and (2) to provide practical drafting and litigation tips on issues that may arise in these areas.

HISTORY OF GOVERNANCE OF INTANGIBLES

Many facets of the law impact the general area of intangible assets. At the federal level, statutes governing patent, trademark, and copyright have existed for many years. In a product-driven, industrial economy, the systems arising under these statutory schemes proved adequate to protect much of the intellectual property issues of the day. However, over the past twenty years, the rapid rise of "soft" assets to the fore of the nation's economy has rendered much of the protection offered by these statutes ineffective or misplaced. Patent covers "invention," which historically has connoted a tangible item. Copyright protects expression only, not ideas or concepts. Trademark protects identification of the source of goods or services. Thus, while the scope of the federal statutory scheme is fairly broad, it does not cover many key aspects of business in today's world, including a great deal of research and development information, technical innovation, processes, business strategy, customer identity information, and "relationship capital" with existing suppliers and customers.

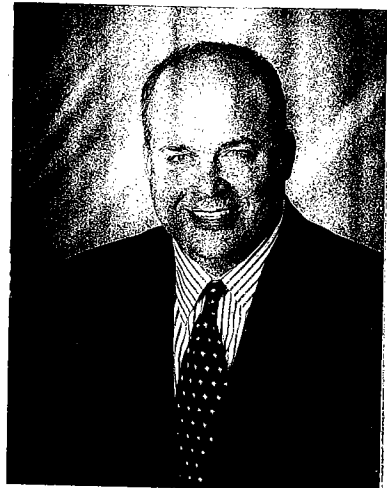
As business has increasingly recognized the real world value of such information, the law has developed to govern many of the issues that arise outside of the historical areas covered by federal statute. The two major areas falling outside the patent, copyright, and trademark scheme are trade secrecy and competitive restrictions. Both have seen rapid development in the United States in the recent past.

Because states such as Colorado (which has enjoyed a large increase of technology-based business activity) have seen a disproportionately large number of issues in this arena, they have led the way in the development of law to cover these areas.

Much of this legal development has been via the typical common-law vehicles, but statutory attempts to deal with these areas have occurred as well. This is especially true in Colorado, which has not only adopted the Uniform Trade Secrets Act ("UTSA"),¹ along with the majority of other states, but has taken the unique step of enacting a statute that governs issues arising as to covenants not to compete (to be discussed in Part II of this article).²

THE MODERN LAW OF TRADE SECRECY

Colorado has long recognized and protected trade secrets. With the adoption of the UTSA in 1986, the law of trade secrecy in Colorado underwent significant revision.



John F. Reha, Littleton, is a partner in the firm of Arckey & Reha, L.L.C.—(303) 798-8546. Reha has a general business practice with an emphasis on intangible asset protection issues.

Common-Law Misappropriation

Prior to the adoption of the UTSA by the Colorado General Assembly, effective July 1, 1986, Colorado adhered to the common-law rule of trade secrecy. At common law, a six-part analysis, set forth as follows in *Porter Industries, Inc. v. Higgins*,³ determined the existence of a trade secret:

(1) the extent to which the information is known outside the business, (2) the extent to which it is known to those inside the business, *i.e.*, by the employees, (3) the precautions taken by the holder of the trade secrets to guard the secrecy of the information, (4) the savings effected and the value to the holder in having the information as against competitors, (5) the amount of effort or money expended in obtaining and developing the information, and (6) the amount of time and expense it would take for others to acquire and duplicate the information. . . . The most commonly accepted definition of trade secrets is restricted to confidential information which is not disclosed in the normal course of exploitation.⁴

Misappropriation Under the UTSA

By its express terms, the UTSA sets forth four elements necessary to establish a claim for trade secret misappropriation: secrecy, value, protective measures, and improper means of appropriation. The first three of these elements are set forth in the definition of trade secret, and the fourth is included in the definition of misappropriation.

Definition of "Trade Secret"

Section 102(4),⁵ which defines trade secret for purposes of the UTSA, varies significantly from the common-law test:

"Trade secret" means the whole or any portion or phase of any scientific or technical information, design, process, procedure, formula, improvement, confidential business or financial information, listing of names, addresses, or telephone numbers, or other information relating to any business or profession which is secret and of value. To be a "trade secret" the owner thereof must have taken measures to prevent the secret from becoming available to persons other than those selected by the owner to have access thereto for limited purposes.

Three elements exist in this statutory definition—secrecy, value, and protective

measures. While these elements are factors in the common-law test, they are *requirements* under the UTSA. Despite this distinction, Colorado courts have continued to cite authoritatively to the common-law test in cases determined after the adoption of the UTSA.⁶ The existence and scope of protective measures as a requirement has served as the key issue in at least two cases decided after the UTSA's adoption.⁷ From these cases, as well as from the language of the UTSA itself, it is clear that secrecy, value, and protective measures are all required for a trade secret to be found.

Secrecy: The "laundry list" of candidates for trade secrecy in the UTSA includes: "any scientific or technical information, design, process, procedure, formula, improvement, confidential business or financial information, listing of names, addresses, or telephone numbers, or other information,"⁸ provided that such items are truly secret.⁹ Secrecy is often the key issue under the UTSA. In turn, the UTSA puts great weight on protective measures as a means of establishing secrecy.

Although the UTSA nowhere requires a written agreement to preserve trade secrecy, enforcement of an oral agreement is by no means a certainty, because an oral agreement may not be an adequate protective measure, except perhaps as to highly technical, clearly proprietary information. If a written employment agreement is entered into that *does not* set forth trade secrecy language, an attempt at imposing a trade secrecy restriction may be barred by the parol evidence rule, especially if the written agreement includes an integration clause. As a matter of general contract law, such clauses typically bar the introduction of evidence in addition to the express terms of the written agreement itself.¹⁰

Protective Measures: For a trade secret to arise under the UTSA, the owner of the information must adopt "measures to prevent the secret from becoming available to persons other than those selected by the owner to have access thereto for limited purposes."¹¹ In *Network Telecommunications, Inc. v. Boor-Crepeau*,¹² the plaintiff's complaint alleged that "contact lists" used by telemarketers were handed out on a weekly basis, telemarketers were prohibited from sharing their lists with co-workers, and the lists were collected and shredded on a regular basis. This was found at least to merit the presentation of evidence on a motion for preliminary injunction.

Conversely, in *Colorado Supply Co. v. Stewart*,¹³ neither a written trade secrecy agreement nor any other appreciable measures were used to safeguard secrecy. Moreover, the "employee" at issue (in fact an independent contractor sales representative) developed much of the information himself, and the information compiled by the "employer" was routinely given to him. As the court stated:

Here, the trial court concluded that plaintiff's customer lists were not trade secrets because: (1) the information was developed by Stewart, who was an independent contractor, rather than by plaintiff; (2) the names on the list can be obtained fairly easily, by reading through the business section of the telephone directory and by asking prospective customers from whom they purchase certain products; and (3) there was no exclusivity as to customers, in that customers purchased the products from more than one vendor. . . .¹⁴

This was found insufficient to confer trade secrecy status.¹⁵

Information that is known generally from observation or that may be developed through means available to the public is not secret and, therefore, cannot be a secret,¹⁶ nor is an employee's pre-existing knowledge.¹⁷ In *Stewart*, the fact that the allegedly confidential information was given to an independent contractor was critical. The Court of Appeals stated:

The trial court also found that the precautions taken to protect all of this information were not those taken to protect trade secrets—they were only normal business precautions. Furthermore, dissemination of this information was not limited to certain employees. Even independent contractors, who were hired as salespersons, were provided the information.¹⁸

Thus, the question arises as to whether maintaining confidentiality of customer lists with independent contractors is even possible. By definition, releasing customer lists to independent contractors allows the information to be known beyond the organization seeking trade secret protection. The court in *Stewart* was of the opinion that releasing customer lists to independent contractors is not consistent with "measures to prevent the secret from becoming available to persons other than those selected by the owner to have access thereto for limited purposes" within the UTSA.¹⁹ Instead, the acts taken by the employer were deemed as "only normal business precautions," which were not

enough to meet the protective measures standard of § 102(4) of the UTSA.²⁰

Stewart is a customer list case, and unlike customer identity, technical and research information usually is considered inherently confidential. Sharing this type of information with independent contractors (especially if such disclosure is done under non-disclosure agreements) may not cause a finding that trade secrecy is lost. Disclosure of such information in this nature is both necessary and routine. It is therefore uncertain that a court would invalidate trade secrecy on such disclosure. A written non-disclosure agreement alone may be a satisfactory protective measure for such information. However, *Stewart* at least raises a question as to whether such an agreement, without more, will render a customer list a trade secret, especially in relation to an independent sales representative.

Value: In the Colorado cases discussing the UTSA, the element of value is rarely noted as an issue. If information has recognized value or if its use would give a competitor an advantage, value would appear to be established.

Element of Improper Means

Aside from the elements found in the definition of trade secret, the additional element of "improper means" must be established for an actionable claim to exist under the UTSA. Such an element arises from the statutory definition of "misappropriation":

"Misappropriation" means:

- (a) Acquisition of a trade secret of another by a person who knows or has reason to know that the trade secret was acquired by improper means; or
- (b) Disclosure or use of a trade secret of another without express or implied consent by a person who:
 - (I) Used improper means to acquire knowledge of the trade secret; or
 - (II) At the time of disclosure or use, knew or had reason to know that his knowledge of the trade secret was:
 - (A) Derived from or through a person who had utilized improper means to acquire it;
 - (B) Acquired under circumstances giving rise to a duty to maintain its secrecy or limit its use; or
 - (C) Derived from or through a person who owed a duty to the person seeking relief to maintain its secrecy or limit its use; or
 - (III) Before a material change of his position, knew or had reason to know

that it was a trade secret and that knowledge of it had been acquired by accident or mistake.²¹

Few Colorado cases feature the improper means element. However, based on *Gold Messenger, Inc. v. McGuay*, it is clear that the use of information by a person in a close relationship with a person under a written trade secrecy restriction setting forth such information as proprietary is actionable.²²

No Statute of Frauds

The UTSA nowhere requires that trade secrecy restrictions be reduced to writing. Assuming that the information is secret and of value, and assuming further that improper means were used to appropriate such information, the lack of a written agreement may not necessarily be fatal to finding misappropriation of a trade secret. Instead of an express requirement of a written trade secrecy agreement, UTSA § 102(4) requires the party asserting misappropriation to have taken "measures to prevent the secret from becoming available to persons other than those selected by the owner to have access thereto for limited purposes." Although a written agreement is not expressly required under such language, it is hard to imagine a situation where a court would prohibit use of certain allegedly proprietary information without such an agreement at least serving as the basis of the trade secrecy claim.

In that regard, the defendant in *McGuay*,²³ although not a party himself to a written agreement providing that certain information was a trade secret, was in a close personal relationship with someone who was a party. Thus, a written agreement served as the ultimate source of the Court of Appeals' opinion in that matter. Included in the cases that have arisen under the UTSA in Colorado are those that feature information such as customer lists.²⁴ The confidentiality of such information appears somewhat suspect under the cases and, without at least a clear showing of reasonable protective measures in the circumstances, trade secrecy will likely be denied. Thus, although a written agreement is not expressly required under the UTSA, it is doubtful that an employer not having such an agreement will be successful in gaining a remedy for use of customer list information.²⁵ Due to their inherently proprietary nature, however, research and development information, internal analyses, future forecasting, and business plans, for example, are more likely to be deemed trade secrets without a written agreement.

Remedies

Remedies under the UTSA include the following:

Actual Damages: Under UTSA § 104(1),²⁶ "damages may include both the actual loss caused by misappropriation and the unjust enrichment caused by misappropriation that is not taken into account in computing actual loss."

Royalty Imposition: As an alternative to actual damages, "a reasonable royalty" may be imposed under UTSA § 104(1).²⁷

Exemplary Damages: Exemplary damages, not to exceed actual damages, may be awarded under UTSA § 104(2)²⁸ "(if the misappropriation is attended by circumstances of fraud, malice, or a willful and wanton disregard of the injured party's rights and feelings."²⁹

Injunctive Relief: Injunctive relief is available under UTSA § 103.³⁰

Attorney Fees: Under UTSA § 105,³¹ attorney fees are available to a defendant if a misappropriation claim is made in bad faith, if a motion to terminate an injunction is made or resisted in bad faith, or if the misappropriation is found to be willful and wanton.³²

Protection of Secret Information: UTSA § 106³³ gives a court the power to protect the secret nature of the information in issue, by, *inter alia*, appropriate protective orders.

Limitations

The UTSA contains its own statute of limitations. UTSA § 107³⁴ requires all misappropriation claims to be brought no later than three years after the misappropriation is discovered or, through the exercise of reasonable diligence, should have been discovered. Section 107 also provides that a continuing misappropriation is to be considered as one claim. Accordingly, the running of the limitations period will not commence until the use of the misappropriated information ceases.

Preemption of Non-UTSA Trade Secrets Claims

UTSA § 108³⁵ sets forth an express preemption provision:

Effect on other law.

- (1) Except as provided in subsection (2) of this section, this article displaces conflicting tort, restitutionary, and other law of this state providing civil remedies for misappropriation of a trade secret.
- (2) This article does not affect:
 - (a) Contractual remedies, whether or not based upon misappropriation of a trade secret;

