

Preserving Your Revenue-management System as a Trade Secret

BY SHERYL E. KIMES AND PAUL E. WAGNER

Make sure that your revenue-management system is safe from trade-secret piracy.

The 1990s saw the wide implementation of sophisticated revenue-management systems in the hospitality industry, made possible by the development of computer technology. These systems involve considerable investment of financial and human resources. Based on our interviews with revenue-management employees from various hotel companies, we are concerned that hotels are not taking sufficient steps to protect their revenue-management systems from misappropriation by their former employees and, by extension, their competitors. This article examines how revenue-management systems can be protected as trade secrets and offers some tips to keep them from getting into the wrong hands. Most of the revenue-management employ-

ees whom we interviewed were not required to sign any kind of confidentiality agreement that specifically protected their employers' revenue-management systems. In this article we discuss how to prevent breaches of hotels' revenue-management systems by protecting them as trade secrets.

Revenue management, defined. Used most commonly by airlines and hotels, revenue management involves matching the supply of a perishable commodity with the demand for that commodity by using strategies that manipulate the price and timing of consumption. One popular expression of this concept is "the application of information systems and pricing strategies to allocate the right capacity to the right customer at the right place at the right time."¹ The determina-

tion of “right” entails achieving both the most revenue possible for the hotel while also delivering the greatest value or utility to the customer. Companies implementing revenue management report increases in revenue of 2 to 5 percent over the results of prior procedures.² In practice, revenue management has meant setting prices according to predicted demand levels so that price-sensitive customers who are willing to purchase at off-peak times can do so at favorable prices, while price-insensitive customers who want to purchase at peak times will be able to do so as well.

Many fingers in the pie. A variety of employees work with revenue-management systems. At the most elementary level, reservation agents quote rates based on the recommendations from the revenue-management system. At the supervisory level, hotels typically have one person in charge of revenue management (either a designated revenue manager or another employee who handles revenue management in addition to other responsibilities). The revenue manager has direct access to the revenue-management system and can override the system’s recommendations if warranted. In addition, some hotel chains (notably Hilton, Marriott, and Starwood) also manage revenue at the regional level and have regional revenue managers who are responsible for multiple hotels. Finally, corporate revenue-management departments employ technical and managerial personnel to assist with the deployment and improvement of their revenue-management systems.

Hotels with successful revenue-management systems clearly convey their pricing strategy to customers. Since revenue management depends on demand-based pricing, it is essential that customers understand which prices are available and what it takes to obtain discounted rates. Successful hotels use “qualified” rates (often referred to as rate fences) which require that customers must meet certain restrictions to receive a discount.

RM Systems as Trade Secrets

“Trade secret” is a legal term that describes a proprietary process, formula, device, or compilation

of information that is used by a particular business. In the United States, the law of trade secrets has developed on a state-by-state basis, although most state trade-secret laws closely resemble each other. As explained below, trade-secret laws set forth certain criteria that define when a business process merits trade-secret status. When met, those criteria allow the owner of a trade secret to prevent others from improperly taking and using those business processes.

Most revenue-management systems used in the hospitality industry could be considered trade secrets if their owners took proper steps and precautions to make them so.³ To that end, owners of such systems should understand the prerequisites to trade-secret protection and actively take steps to ensure that those prerequisites are met. Stated in the negative, an owner’s failure to take the necessary steps and precautions may cause its valuable revenue-management system to fall into the public domain, where its competitors are free to use the system without restriction.

The third edition of *Restatement of Law* defines “trade secret” as “any information that can be used in the operation of a business or other

Most revenue-management systems used in the hospitality industry could be considered trade secrets.

enterprise and that is sufficiently valuable and secret to afford an actual or potential economic advantage over others.”⁴ This definition is usually broken down into two required elements, namely, value and secrecy.

Value. The element of value simply requires that the trade secret be sufficiently valuable to provide an actual or potential economic advantage over others who do not possess the information. The advantage need not be great, but it must be more than trivial. The mere use of a trade se-

² See: *Ibid.*; and Richard D. Hanks, Robert G. Cross, and R. Paul Noland, “Discounting in the Hotel Industry: A New Approach,” *Cornell Hotel and Restaurant Administration Quarterly*, Vol. 33, No. 1 (February 1992), pp. 15–23.

³ Certain elements of revenue-management systems may be subject to other forms of intellectual-property protection, such as patents, and therefore may not be eligible for trade-secret protection.

⁴ *Restatement of the Law*, third edition, Unfair Competition, § 39, The American Law Institute (1995).

cret in one's business is evidence of its value, and so are tangible benefits realized by the owner through use of the trade secret, such as an identifiable increase in revenue. Other evidence of value includes the willingness of others to pay for a right or license to use the trade secret, and the amount of resources invested in the research and development or protection of the trade secret.

The fact that revenue-management systems have value is easily established, in part because the purpose of these systems is to maximize revenue from a hotel or group of hotels. Since revenue is measured in detail by the system itself,

Owners of a trade secret must take reasonable steps to keep their materials and information secret from their competitors.

any revenue-management system worth protecting can typically generate the evidence necessary to prove its own value. The claim of revenue-management proponents that a properly integrated system can increase revenues by as much as 5 percent over past practices can be evidence of value. Furthermore, as many hoteliers who have developed these systems will attest, they are expensive to develop, implement, and operate. Thus, the considerable resources devoted to developing and operating revenue-management systems can be used to establish their value to the owner.

Also, successfully implemented revenue-management systems often draw interest from competitors in the form of offers to purchase the system. For example, in a closely watched lawsuit, American Airlines sued Northwest Airlines for misappropriation of American's revenue-management system.⁵ To establish the value of its revenue-management system, American demonstrated, among other things, that Northwest previously offered to purchase American's system after Northwest concluded that the in-house development of its own "next generation" system

would cost as much as \$30 million.

Secrecy. The element of secrecy is the *sine qua non* of trade-secret law. This element requires that owners take reasonable steps to keep their materials and information secret from their competitors. Secrecy need not be absolute. Instead, the element of secrecy is satisfied if, as a result of the precautions taken by the owner, it would be difficult or costly for others who could exploit the information to acquire it without resort to wrongful conduct.⁶ On the other hand, information that is generally known or readily ascertainable through proper means by others to whom it has potential economic value would not be considered to be a trade secret. For example, information that can be easily obtained from trade journals, scientific texts, or other published material lacks the requisite secrecy to qualify as a trade secret. Similarly, information about the nature, design, or manufacture of a product that can be readily ascertained from an examination of the product on public sale or display is not a trade secret. However, public knowledge of some, or even all, of the components of a trade secret does not destroy its trade-secret status if the combination or integration of the known components remains confidential.

The fact of secrecy can be established by evidence that others have tried and failed to duplicate the information by proper means, and also by the willingness of others to pay for the right to use the information. Furthermore, should a competitor wrongfully attempt to acquire a trade secret, such an effort would create an inference that the trade secret is sufficiently inaccessible as to qualify for protection.

Secrecy of information or material must be preserved through the reasonable efforts of its owner. Mere intent to keep information confidential is not enough to preserve trade-secret protection. An owner who fails to take affirmative precautions to protect the proprietary information risks losing trade-secret protection for that information, even if it is initially disclosed through improper means (as we explain next).

Confidentiality. The owner's disclosure of a trade secret to others will not destroy the trade secret's status if the disclosure is made under the

⁵ *Northwest Airlines v. American Airlines*, 853 F. Supp. 1110 (D. Minn. 1994).

⁶ *Restatement of the Law*, Third, Unfair Competition, § 39, comment f, The American Law Institute (1995).

condition of confidentiality. For example, disclosures to employees, licensees, and independent contractors will not destroy a trade secret's protection as long as the information's recipient knows of the confidential nature of the information and agrees not to disclose it to others. In such cases, the law imposes a duty of confidentiality on the recipients of the information, the breach of which constitutes wrongful conduct.

When information is no longer sufficiently secret to qualify for protection, it lapses into the public domain and can be used by others without restriction. Thus, a competitor's otherwise wrongful acquisition of information will not give rise to a legal claim for relief by the owner if the information is no longer secret.

One scenario for how such loss of secrecy could occur might be as follows. Say that the owners of Hotel A confidentially disclose its revenue-management trade secrets to managers at Hotel B during negotiations of a possible licensing agreement. The negotiations break down and no agreement is reached, but Hotel B's managers retain photocopies of the trade-secret information (although they cannot legally use that information). Subsequently, Hotel A's revenue manager discloses the same trade secrets to a job candidate during an interview. That candidate rejects an offer from Hotel A and accepts an offer from Hotel B. Because of Hotel A's unprotected disclosure, Hotel B can now exploit the trade secret without liability, regardless of whether Hotel B extracts the information from its new employee, or relies on the prior confidential disclosure.

Revenue Management as a Trade Secret

Most revenue-management systems in the hospitality industry can qualify as secret because the bulk of their components and the systems as a whole are not ascertainable through public sources. The typical revenue-management system comprises a number of integrated computer-based systems that rely on a mix of publicly available data and hotel-specific information. Even if some of the components of a particular revenue-management system can be ascertained through the industry literature (e.g., the mathematical models used to forecast bookings), the integration of those components into the larger system is not.

In *Northwest Airlines v. American Airlines*, for instance, Northwest argued that American's revenue-management system could not qualify for trade-secret protection because it contained information available in the public domain. Specifically, Northwest claimed that the exponential smoothing equations and other features of American's revenue-management system were available in textbooks and industry literature. Although the court acknowledged that certain aspects of American's revenue-management system could be ascertained from public sources, it found evidence that this information did not exist "at a level of specificity which would enable formulation of working applications of the various principles solely from public sources."⁷ The court also noted that Northwest's argument was belied by the fact that it did not obtain information regarding American's revenue-management system from public sources, but rather from American employees willing to disclose the information in detail.⁸

Vigilance. Given that a revenue-management system can be a trade secret, hospitality operators must remain vigilant in preserving their system's secrets. Such vigilance is particularly essential in view of the constant turnover of employees among hospitality enterprises. Perhaps the greatest threat to a system's trade-secret status is that a company's former employees may be

Hotels with strong revenue-management systems may find that competitors are trying to learn their secrets.

tempted to disclose the essential points of that company's revenue-management information to a subsequent employer. Indeed, the occasion arises that hotels with less-developed revenue-management systems will raid the revenue-management departments of hotels with mature, successful systems by luring key employees away with more lucrative salaries and benefits.

⁷ 853 F. Supp. at 1114.

⁸ *Id.*

Thus far, the only reported cases regarding trade-secret infringement appear in the airline industry (as in the case of *Northwest Airlines v. American Airlines*). However, hotel-related cases are likely to crop up for two reasons. First, as certain hotels achieve a level of success with mature, computer-based revenue-management systems (about a decade behind the airlines), other hotels with less-developed systems will look to mine the RM departments of the former, rather than incurring substantial research and development costs to develop independently their own systems. This phenomenon is already occurring, according to a number of hotel RM employees we spoke to while researching this article. Second, the popularity of trade-secret misappropriation lawsuits in the United States is on the rise, as employers discover that these actions are an effective means to gain a competitive edge by curtailing key former employees' abilities to work for the competition.⁹

In the remainder of this article, we present precautions that can be taken to maintain trade-secret protection and reduce the risk that employees will actually disclose confidential information either during or after employment. The precautions that we recommend also improve a hotel's chances of successfully litigating a claim of trade-secret misappropriation if confidential information is disclosed by an employee and used by a competitor.

Preserving the Confidentiality of Revenue-management Systems

Hotel companies should implement specific policies and procedures to protect revenue-management trade secrets. To begin with, each company's situation is distinctive, and therefore legal counsel should review specific trade-secret policies and procedures. Following is a list of precautions that all hotel companies should consider.

Physical security. Confidential revenue-management information should be kept secure from hotel guests and other non-employees. Furthermore, employees' access to this information

should be permitted only on a need-to-know basis. Offices and file drawers containing revenue-management information should be kept locked, and computer files containing this information should be password protected. Likewise, communications containing confidential information should occur only over secure telephone lines or computer networks. E-mail messages containing confidential revenue-management information that are vulnerable to interception should be encrypted, with the code given only to the intended recipients.

Restrictive legends. Documents and computer files containing confidential information should be conspicuously marked with restrictive legends such as "Confidential—Trade Secret Information," and "Restricted Access—Do not copy or distribute outside this company." Restrictive legends accomplish two important goals. First, they instruct intended recipients of the information that the document or computer file is confidential, and the legends continue to reinforce that message each time the recipient views the information. Honest employees who are repeatedly reminded of the confidential nature of the information are less likely to disclose it. To the extent an employee wrongfully discloses the information, moreover, these restrictive legends allow the hotel to rebut any claim by the employee that he or she was unaware of the confidential nature of the information at the time of the disclosure.

Second, restrictive legends instruct unintended recipients that the information is confidential and not meant for their review. In the case of an accidental disclosure to an unintended recipient, restrictive legends make it less likely that the recipient will misappropriate or otherwise use the information. In the case of an intentional misappropriation by a competitor, restrictive legends probably will not dissuade the competitor from using the information, but those legends will improve a hotel's chances of demonstrating that the competitor knew that the information was a protected trade secret.

For particularly sensitive documents, employers should distribute only a limited quantity of serially numbered copies, with a record of each recipient by number. This will increase the chances of tracing an unintentional or wrongful disclosure of the document.

⁹ See: Michelle Singletary, "Some Employers Would Rather Fight Than Let You Switch; Defections Bring Court Cases Against Key Workers, Recruiting Companies," *The Washington Post*, May 14, 1997.

Employee handbooks. Employee handbooks should state a confidentiality policy that specifically lists revenue-management information as a trade secret and provides detailed instructions to prevent disclosure. Further, the handbook should instruct that confidential revenue-management information will be shared only with authorized employees who have had the proper training and signed a confidentiality agreement.

Confidentiality agreements. Before beginning to work with revenue-management information, all employees with access to the system should sign a specific confidentiality agreement regarding that information. Such agreements should contain an acknowledgment by the employee of the confidential and proprietary nature of the information, an express agreement to preserve its confidentiality and report any unauthorized disclosure of it, an acknowledgment that the employee's duty to preserve the confidentiality of the information continues after the employment relationship has ceased, and an agreement to return all documents and materials containing confidential information at the end of the individual's employment.

Confidentiality agreements are effective in two distinct ways. First, by identifying the revenue-management information as a trade secret as part of the confidentiality agreement,¹⁰ the employee's express acknowledgement of this fact rebuts any later claim by the employee that he or she did not know of the confidential nature of the information. This has great evidentiary value in a lawsuit against such an employee for misappropriation of trade-secret information. Second, to the extent that the confidentiality agreement possesses consideration, it can be enforced as a legally binding contract. Consideration simply requires that each party to a contract give something up in exchange for what the other gives up. A confidentiality agreement requires an employee to give up the right to disclose or use the employer's trade-secret information. Whenever

possible, an employer should "give something up" in exchange for an employee's promise of confidentiality. The employer may "give up" the employee's initial employment (that is, hire the person), a promotion, a raise, or a bonus.

State laws differ as to whether continued employment alone is sufficient consideration for an employee's promise of confidentiality. In Minnesota, for example, a promise not to disclose trade secrets is not enforceable as a contract if

Hotels should specifically label the materials supporting their revenue-management systems as confidential.

the employee signs it after employment has already commenced, because continued employment alone does not constitute valid consideration.¹¹ In other states (e.g., Indiana), however, continued employment and payment of wages is valid consideration for an employee's promise of confidentiality. The ability to enforce the confidentiality agreement as a legally binding contract gives an employer an additional claim, namely, breach of contract, against an employee who misappropriates trade-secret information.

Employee training. Employees should receive thorough training and repeated reminders of the confidential nature of the revenue-management information, the steps to ensure preservation of its trade-secret status, and the employees' obligation to protect the information from disclosure. Training should begin when employees are first hired to work with the revenue-management system and should be incorporated into the substantive revenue-management-orientation process. Meetings should be held no less than annually to remind employees of their legal obligations to their employer. These meetings should include written handouts that can later be used as evidence to demonstrate an employee's knowledge of the proprietary and confidential nature of the information.

¹⁰ Indeed, these agreements should specify what information and materials within the revenue-management system constitute the company's trade secrets, because an agreement that prohibits employees from disclosing trade secrets may not be enforceable if it does not specify what those trade secrets are. See: Kurt H. Decker, *Covenants Not to Compete*, Second Edition, Volume 1 (New York: John Wiley & Sons, 1993), p. 92.

¹¹ See: *Freeman v. Duluth Clinic, Ltd.*, 334 N.W.2d 626 (Minn. 1983).

Exit interviews and reminder letters. When an employee with access to revenue-management information is terminating employment, managers should meet with that employee and ask the person to acknowledge her or his ongoing obligations to their employer in writing. The written document signed by exiting employees should acknowledge the confidential nature of the company's revenue-management information, the employees' continuing legal and contractual obligations to keep the information secret, and the fact that they no longer possess any documents or materials containing confidential revenue-management information. The departing employees should be advised in writing that any subsequent disclosure of this information would violate their legal obligations to their employer and subject them and possibly the information's recipient to legal action. An employee who refuses to acknowledge these things in writing by initialing an appropriately worded document should be closely watched. In addition to an exit interview, the former employer should send a letter to all exiting employees to remind them of their legal obligations, with an

ality of those trade secrets and agreed not to disclose them (attaching copies of all written agreements and acknowledgments), and that any disclosure of confidential information would be met with appropriate legal action. Such a letter would put the new employer on unequivocal notice of a company's claim of trade-secret protection and eviscerate any potential claim by the new employer that a disclosure and use of secret information is unintentional.¹² However, such letters come with certain legal risks, and so a company should consult with legal counsel before taking this step.¹³

Human-resources Considerations of Trade-secret Protection

Many employers are reluctant to require their newly hired employees to sign confidentiality agreements and other restrictive covenants because they feel such agreements set the wrong tone for the employment relationship. At a minimum, some employers believe these agreements create an atmosphere of distrust. At worse, restrictive covenants may cause a potential employee to refuse an otherwise acceptable job offer. While these are valid concerns, the absence of confidentiality agreements significantly increases the likelihood of an unprotected disclosure, and the resulting loss of trade-secret protection.

A prudent policy would be to require confidentiality agreements and to take the other precautions set forth above, while at the same time acknowledging employees' fears and taking steps to allay those fears. First, employers should emphasize the positive aspects of the company's confidentiality policies, such as the tremendous value of the company's trade secrets, the competitive advantage resulting from those secrets, and the

A prudent course would be to have revenue-management employees sign a confidentiality agreement.

enclosed copy of the company confidentiality policy, the employee's confidentiality agreement, and the written acknowledgment by the employee at the exit interview, if available.

Advisory letter to new employer. While this step may not be appropriate in every case, in certain circumstances one could send an advisory letter to the new employer of a former employee. For example, a revenue manager who quits to take the same or similar position with a competitor is more likely to possess detailed trade-secret information and has the potential of using that information for the benefit of the competitor. The letter should advise the new employer that the employee was privy to all of the company's revenue-management trade secrets, that the employee acknowledged the confidential-

¹² If a third party obtains a trade secret from a former employee whom the third party knows has disclosed the information in breach of a restrictive covenant or duty of confidentiality, the third party will bear liability for the misappropriation. See, for example: *A.H. Emery Co. v. Marcan Prods Corp.*, 268 F. Supp. 289 (S.D.N.Y. 1967), *aff'd* 389 F.2d 11 (2d Cir.), *cert. denied*, 393 U.S. 835 (1968).

¹³ A letter to a former employee's new employer may give rise to a claim by the employee of tortious interference with the employee's contract with the new employer, or worse, defamation. Because of these risks, the wording of such a letter is critical and should be approved by legal counsel.

fact that the employee is trusted enough to work with such sensitive information. Second, the employer should point out that the confidentiality agreements are not non-competition agreements and therefore do not restrict an employee from any future employment; they merely prohibit the employee from disclosing company trade secrets either during or after the employment relationship. To emphasize this point, the employer should specifically identify the various materials and information that are trade secrets so the employee understands precisely what is covered by the confidentiality agreement.

Be proactive. If your hotel does not have in place precautions like the ones we suggest here, we urge you to take appropriate precautions to protect your revenue-management system immediately before any unintended disclosure occurs. The hotel that implements these policies and procedures only in reaction to a disclosure by a former employee may find itself unable to put the genie back in the bottle. ■



Sheryl E. Kimes (at left) is an assistant professor of quantitative methods at the School of Hotel Administration at Cornell University. **Paul E. Wagner** (at right), is an adjunct professor of law at the School of Hotel Administration at Cornell University and a partner at Stokes & Murphy, a law firm providing labor and employment advice to clients in the hospitality industry.