

Protecting your rent-to-own trade secrets

Last February, the Poneman Institute reported the startling results of a survey of employees who had left their jobs during the past year. Nearly 50 percent took proprietary information belonging to the employer on their way out the door. Two-thirds took e-mail lists. Nearly half took non-financial business information. Forty percent took customer contact lists. A third took employee records. Two-thirds said that they took the information to get a leg up on a new job. Twenty-five percent said that they still had access to their former employer's computer network after having been terminated.

Those conducting the survey conjectured the causes of such behavior to be increased employee mobility, a lack of employee loyalty to an employer and an increased sense of employee entitlement to information that really belongs to the employer.

BY ED WINN III

One can only wonder whether statistics among rent-to-own employees would be better or worse than these national averages. Rent-to-own employees are probably more mobile than average. Whether they are more or less loyal probably depends upon the employer. It would come as no surprise that an RTO employee might view himself as more valuable to a competitor down the street if he showed up for the job interview with his former employer's customer list.

There are laws in place to protect a company's trade secrets and other proprietary information. Most states have criminal theft-of-trade-secrets statutes, modeled on the *Uniform Trade Secrets Act*. There is a federal criminal statute, the *Economic Espionage Act of 1996*, with penalties of up to \$500,000 for individuals, up to \$5 million for companies and up to 10 years in the penitentiary. These statutes apply to the employee thief and can also apply to a competing company that knowingly and intentionally obtains and uses the trade secrets of another company.

Today, there may not be many secrets in a rent-to-own store—a lot of people know how to rent and collect, after all. RTO stores and their software systems generate reams of reports that measure store performance. In addition, there are financial records, product lists, strategic plans, training manuals, policy and procedures manuals, and more. All of this information is proprietary in the sense that the employer uses it to run the store and would prefer that the competition not have access to any of it. Whether some of this information rises to the level of trade secrets can be a complicated legal issue. Customer files, however, are generally perceived by dealers as secret and valuable. When a dealer sells a store, the customers and their files are primarily what he or she is selling. That is where the value lies in such a transaction, far outweighing the value of the trucks, fixtures, equipment and idle inventory.

Distinguishing between what is a true trade secret and what is merely confidential or proprietary is important. If a dealer were to mark every report as a trade secret, it could weaken the argument that a stolen customer list is really a trade secret. Also, rental dealers must distinguish between trade secrets and the general knowledge, skill and experience an employee gains on the job—courts make that distinction, protecting the former, but not the latter.

What is a trade secret, then? The general definition is: any valuable business information that is kept confidential in order to give the business a commercial advantage in the marketplace and that cannot be obtained readily from publicly available sources. A key element in the definition is whether the employer has taken steps to keep the information secret. That means protocols such as keeping customer files in a locked filing cabinet and limiting who has access to them. It means marking the files as “TRADE SECRETS: DO NOT COPY.” It means having control of logs to see who accesses the files. It includes using passwords, if some of the information is stored electronically, and changing those passwords when an employee leaves the company.

In an Alabama case, the state supreme court ruled that a customer list was not a trade secret because the company had not taken sufficient steps to maintain secrecy: “At least 10 employees had free access to the lists. In addition, the lists were not marked ‘Confidential;’ the lists were taken home by employees; multiple copies of lists existed and the information was all in the receptionist’s Rolodex file.” (*Allied Supply Company v. Brown*, 585 So2d 33, Alabama 1991.)

Often, a former employee’s misdeed will become apparent to the ex-employer. The employee goes to work for a competitor and soon thereafter, customers are getting calls from the competitor’s store urging them to return merchan-

dise and do business with the new store. Pursuing a former employee and his or her new employer for stealing your customer list can be time consuming and expensive, and proving your case can be difficult. On similar facts in the Northwest a few years ago, a rental company spent more than \$50,000 in discovery before giving up in disgust. Among other things, when confronted with evidence that he had called customers from his new store, the former employee insisted that he had recalled the phone numbers from memory and not from accessing them off his previous company’s list.

In light of the amount of information that some employees are taking with them when they leave a company, what can rent-to-own dealers do to protect their business’ trade secrets from being compromised? They can require employees to sign confidentiality agreements. These agreements list the items that the employer deems to be confidential or trade secrets. They can be made part of employment agreements or included in the policies-and-procedures manual that the employee signs separately.

Such an agreement should clarify that the employer makes no claim on the employee’s general knowledge, skill or experience acquired while on the job. The agreement should include a promise that the employee will return all written and electronic material considered confidential when employment terminates. For a new hire, get a representation that the new employee is not bringing anything with him into the company in violation of a former employer’s confidential, proprietary or trade-secret information.

Dealers may consider requiring vendors, independent contractors and third parties to sign modified confidentiality agreements if they are going to have access to the company’s proprietary information. The agreement can require the employee to agree to injunctive relief if there is a violation. A confidentiality agreement gives the employer the right to allege “breach of contract,” another weapon—in addition to criminal statutes—to use if the employee runs off with trade secrets. Confidentiality agreements, if carefully drafted, will be enforceable everywhere.

Also, rental dealers can require employees to sign covenants not to compete as a condition of employment, both during employment and for some period after they leave the company; however, non-compete covenants are not enforceable everywhere. California, for example, has determined that such covenants in the employment context are unenforceable because they conflict with an employee’s right to make a living. On the other hand, rent-to-own dealers in other states have been successful in getting injunctions against former employees to prevent them from going to work for a competitor during the term of the covenant.

Covenants not to compete do restrain trade and therefore must be reasonable in terms of 1) how long the covenant lasts;

2) the geographic limits of the covenant; and 3) the type of activity limited by the covenant. In the rent-to-own business, covenants for employees usually last from one to two years after employment ends. Anything longer will be difficult to

getting the departing employee to certify that he is aware of the confidentiality agreement or covenant not to compete and fully intends not to copy, retain, disclose or use any of the company's trade secrets. There are technologies available that allow an employer to create a forensic image of an employee's hard drive to determine what is on it when an employee leaves.

If trade-secret theft is discussed during store meetings from time to time—and if the company's policies regarding private business information are carefully and fully explained at the beginning as well as at the end of the employment—then the rental dealer stands a better chance of keeping his secrets confined to his employees who are supposed to be using them.

Perhaps the most important thing that a rental dealer can do is to increase awareness of the issue of employees taking company information with them when they leave. Put some focus on the problem. If employees never hear about the issue, then they are not likely to be sensitive to its importance. If trade-secret theft is discussed during store meetings from time to time—and if the company's policies regarding private business information are

enforce due to the length of rental agreements and the rate of employee and customer turnover. Geographic limits for store-level employees should conform to a business' delivery area. Employees higher up in the organization may be further restricted, but the narrower a company can draw the geographical limits on an employee, the better the chance that a court will find it to be reasonable and enforce it.

carefully and fully explained at the beginning as well as at the end of the employment—then the rental dealer stands a better chance of keeping his secrets confined to his employees who are supposed to be using them.

By the way, a covenant not to compete that is a part of the sale of a business is treated very differently in the law from employee covenants. In one rent-to-own case, the court enforced a covenant not to compete in a one-store sale that extended out 200 miles from business, based on the ADI of the store location. The court ruled that the seller made the deal and had to live with it.

Advice to employees: you made certain promises to your employer when you took the job and you need to keep those promises or risk severe civil and possibly criminal penalties. First of all, give all of the employer's property back—originals and copies—when your employment terminates. Even if you have not signed a confidentiality agreement or a covenant not to compete, you still cannot take your employers property with you when you leave. You may get your new employer in trouble if you try to use information that you have taken from a former employer. You risk permanent harm to your reputation in the industry.

In employee covenants, proscribed activity must conform to that necessary to protect the former employer's type of business. A general prohibition against the employee continuing in the rent-to-own business might not be enforced if he or she leaves a store that rents televisions, appliances and/or furniture and goes down the street to work in a wheel-and-tire rental store. If an employer goes for too many restrictions, most courts will declare the covenant to be an unreasonable restraint of trade and rule it unenforceable. A minority of courts will modify the covenant to make it reasonable.

Know that the entire history of all e-mails that you have sent on company computers can be retrieved, if necessary. Those e-mails are not necessarily private. Your employer has tools that allow him to recover all of your e-mails, even the ones you have deleted. Employee e-mails have been used by employers to prove wrongful solicitation of the employer's customers, breach of fiduciary duty, conversion and theft.

Also, dealers may want to consider having employees sign a non-solicitation agreement. These agreements prevent a former employee—over a designated period—from attempting to persuade former co-workers to come work for the new employer. This agreement should apply both *while* the employee is working and *after* employment is terminated. The agreement also may include the non-solicitation of customers.

Know that the entire record of telephone calls you have made on company telephones can be retrieved. Telephone companies keep records of all calls made for years and, while the substance of those calls may not be available, who you talked to and when is within the companies' databases and is discoverable information. *

It is important to have an in-depth exit interview with employees whenever possible. A part of the interview can include

Ed Winn III is APRO's general counsel. His e-mail address is edwinn@mwvmlaw.com.