YOU AUTO KNOW©

July 2013

Robert A. Poklar, Esq.
Weston Hurd LLP
The Tower at Erieview
1301 East 9th Street
Suite 1900
Cleveland, Ohio 44114-1862
p: 216.687.3243
f: 216.621.8369
rpoklar@westonhurd.com
www.westonhurd.com

Follow me on Twitter @YouAutoKnowLaw

Misappropriated Confidential Documents

Scenario:

Your F&I manager has been with you for several years and is a trusted employee. One day, he submits his resignation which takes you by surprise; however, you wish him well. Over the next few weeks, you have current customers calling you regarding mailings and telephone calls they are receiving from your ex-employee. In fact, your neighbor tells you that he received a call on his private cell phone and was not happy. After investigation, it becomes apparent that your alleged loyal ex-employee downloaded your customer base, including confidential information. He further took your entire business and advertising plan for the year. What are your legal rights?

If you have been in the retail auto business for more than a few days, you know that this happens on a frequent basis. Perhaps not to the extent as the facts in the scenario, but frequently with salespeople taking customer lists. This author has provided advice and has litigated numerous situations as described in the scenario.

First, you have legal recourse against the unscrupulous employee. But first make sure your own policies and procedures are in place. This will strengthen your case. What efforts has the dealership taken to protect its confidential and proprietary information? You will want to show the Judge that the dealership took serious efforts to protect its information, and be able to demonstrate that the efforts were generally successful. For example and this list is not exhaustive, I suggest that you start with your employee handbook. It should have a section that deals with company and customer information that states that any such information is confidential and proprietary to the dealership and cannot be disseminated or used for personal purposes. Further, you have policies in place to comply with the "Red Flag" rules. The access to certain computer information and programs needs to be limited and password protected. Remember, you are not

only protecting your database and information, but the confidential information of your employees and customers. You do not want to be in a position where you have to notify your customers that their personal information has been compromised.

Once you determine that your ex-employee has taken the information, what can you do? First, send a cease and desist letter to the ex-employee and, if necessary, to his/her current employer demanding that all information be turned over or destroyed immediately or litigation will ensue. After this fails, because the typical response is that only the ex-employee's "personal" customers were contacted, you need to file litigation. Again, remember, unless the employee specifically provided you with a list of his/her prior customers at the time of hiring, those customers are the property of the dealership. It is important to note that information that is available through other third party sources is not protected. For example, a customer's address and telephone number which is available in a telephone book or via a Google search or the cost of a vehicle which one can reasonably find out on the internet, are not protected. However, personal customer information, pricing policies, future advertising and business plans, customer lists, sales, lease, service documents, financial information of the business, to name a few, are protected.

The litigation process begins by filing a lawsuit claiming a breach of trade secrets, theft of business records, perhaps a claim under the Computer Fraud and Abuse Act, breach of fiduciary duty, and violations of the state secret protection laws. There are other causes of action that can be used depending on the facts and circumstances. The only problem is that damages are typically difficult to prove. Therefore, it is essential that a demand for a Temporary Restraining Order and Request for a Preliminary and Permanent Injunction be included. Typically, when the court grants the Motion for a Temporary Restraining Order, the parties generally, at the court's insistence, will attempt to come to an early resolution.

The final outcome depends on the type of information which was compromised. Generally, the ex-employee will agree to turn over any information taken and agree to cease his or her activities. This may include an agreement that if the ex-employee continues the illicit action, monetary damages will automatically be imposed. This is serious litigation and you have to make sure you have all your facts in place.

CONTACT INFORMATION
Robert A. Poklar, Esq.
Weston Hurd LLP
The Tower at Erieview
1301 East 9th Street, Suite 1900
Cleveland, Ohio 44114-1862
p: 216.687.3243; f: 216.621.8369
rpoklar@westonhurd.com
www.westonhurd.com

As always, these are highlights of the law and are not to be construed as containing the entire law. This is not to be construed or relied upon as a legal opinion. If you are presented with this problem, contact your legal counsel for advice.

Having been a Chevrolet dealer, Robert A. Poklar's business background and experience in the automotive industry aid him in his representation of numerous Ohio automotive dealerships. He also represents after-market service companies, trade organizations, dealers, advertising associations and corporations. Pursuant to certain ethical standards, this may be construed as advertising.