

# SMART BUSINESS<sup>®</sup>

INSIGHT. ADVICE. STRATEGY.™

DALLAS

## SMART LEADERS

How Rick Davis gets around the hiring roadblock to grow DAVACO

## FAST LANE

How Bridgefarmer's Mansoor Ahsan builds relationships with clients and employees

# Strength in numbers

HOW DOUG HAWTHORNE  
MERGED 13 HOSPITALS AND 18,000  
EMPLOYEES TO BUILD A NEW  
ORGANIZATION FROM SCRATCH

# Keep your lists safe

Protect customer lists as trade secrets. **Interviewed by Curt Harler**

**F**ew assets are as important both to a company's sales efforts and to maintaining good customer relations as its list of client names and data. Lose the list and you give away much of the proprietary information that you built up during the years of working with the customer. Your firm stands to lose face — and business — if the list is stolen and used by others to undercut your business. When possible, customer lists should be protected as trade secrets, says J. Robert Arnett II, an attorney with the Dallas law firm of Munck Butrus Carter, P.C.

## Are all client lists protectable as trade secrets?

Not by a long shot. First, they have to be secret. That does not require an absolute secret — known to one person and one person only — but it does mean the information cannot be well-known or easily acquired in the trade or industry. Second, they have to derive value or at least potential value from the fact that the information is not generally known or easily acquired. In other words, the fact that you have the information and your competitors do not gives you a competitive advantage. Third, the owner has to take reasonable efforts to maintain the secrecy of the list, which includes physical security and educating employees about their obligation to keep the information confidential. If customer lists are legitimate trade secrets, courts will give them a high level of protection.

## How can a firm protect its customer lists?

First, you can employ physical security measures — keeping the lists secured, restricting access to the area within your facility where the lists are kept, limiting access to those employees who have a need to know and use them, password protecting files, and limiting access to computer servers where the lists are kept. Second, you can take steps with your existing employees to reinforce the secrecy of the lists by training employees about the



**J. Robert Arnett II**  
Shareholder  
Munck Butrus Carter, P.C.

importance of protecting trade secrets and requiring employees to sign nondisclosure and/or noncompete agreements. Third, you can take steps with departing employees to reduce the risk of them stealing your lists — conducting exit interviews to remind departing employees of their duty to not disclose trade secrets and confidential information, checking what materials the employees are taking with them as they leave, requiring them to leave immediately, retrieving their keys and pass cards, disabling their computer network access, and having them come back after hours to clean out their offices under supervision.

## What about when a trusted employee leaves? A simple jump drive will download an entire hard drive.

You can't completely stop employee theft, particularly when technology exists that makes it easy to copy information. You can minimize the risk by having employees sign nondisclosure and noncompete agreements. Noncompete agreements have to

be reasonable as to duration, scope of prohibited activities and geographic extent, but courts are willing to enforce reasonable noncompetes by issuing injunctions against departing employees. If they can't go after your customers at all for some period of time — say two years — stolen lists have less value to them, and by the time they can compete the stolen list may have lost most of its value. Some firms also employ measures that will alert them if someone has stolen and is using a list, for example, by 'salting' the list with people who are not real customers or prospects and who will inform the firm if someone has contacted them to solicit business.

## Isn't it difficult, even with names 'salted' in a list, to prove a list was stolen?

It is a rare case in which a departing employee admits to stealing a list. Unless you get some direct evidence through discovery, you generally have to rely on circumstantial evidence. But that is broadly true in all types of business litigation and is not a barrier to enforcing your rights.

For example, if a competitor who hired your former employee suddenly contacts your best customers and undercuts your prices, that is pretty good circumstantial evidence it is using your list. And, if a competitor calls a 'salted' name — like your uncle who is not in the relevant market — it is hard to envision the competitor coming up with an innocent explanation. That's very good evidence, even if it is circumstantial.

You may also be able to get direct evidence that the competitor has your list through aggressive discovery, including seeking a forensic examination of your competitor's electronic files. That can be expensive, but if the list you are trying to protect is valuable it can be worth the effort and expense. <<

**J. ROBERT ARNETT II** has more than 20 years of experience in all aspects of civil litigation at trial and appellate levels in state and federal courts as well as before domestic and international arbitration tribunals. A shareholder at the Dallas law firm of Munck Butrus Carter, P.C., 100 percent of his practice is devoted to litigation. Reach him at [Barnett@munckbutrus.com](mailto:Barnett@munckbutrus.com).

**Insights Legal Affairs** is brought to you by Munck Butrus Carter, P.C.