

PROTECTING CUSTOMER RELATIONSHIPS IN THE BLACKBERRY® AGE

By Benjamin I. Fink, *Berman Fink Van Horn, P.C.* and
Anne E. Andrews, *Berman Fink Van Horn, P.C.**



The proliferation of BlackBerrys®, iPhones and other “smart phones” has complicated what business owners must do to protect their customers’ contact information from being taken and used by departing employees to compete.

It is not an unlikely scenario: FirstCo’s top salesperson, Sally Superstar, leaves the company to work for PoachCo, taking FirstCo’s customers’ names and contact information with her on her personal BlackBerry®. What legal rights does FirstCo have to keep Sally from using its customer information? Can Sally use that information to solicit FirstCo’s customers on behalf of PoachCo.?

If Sally did not sign an agreement containing covenants against the use of confidential information, solicitation of customers or competition while working for FirstCo, FirstCo’s primary avenue for legal recourse may be the law of trade secrets. In Georgia, trade secrets law is embodied in the Georgia Trade Secrets Act (the “GTSA”). O.C.G.A. § 10-1-760, *et seq.* Like Georgia, most other states have similar statutes addressing trade secrets.¹

Under the GTSA, if a company can show that its customer lists, pricing information and other sensitive documents or information are trade secrets, it may be able to prevent a departing employee from taking or using that information in a competitive manner. *See, e.g., DeGiorgio v. Megabyte Intern., Inc.*, 266 Ga. 539, 468 S.E.2d 367 (1996). The key to claiming protection under the GTSA is showing the information constitutes a “trade secret.” This requires proof of several elements. First, a company must show that the information in question belongs to the company. Second, the information cannot be commonly known by, or available to, the public. Third, the information must have actual or potential economic value to the person who possesses it because others cannot generally ascertain it by proper means. And fourth, the company must have used reasonable efforts to maintain the secrecy of the information. O.C.G.A. § 10-1-761. More than anything else, written policies regarding the use and disclosure of sensitive information, as well as policies concerning computer use, are critical to a company’s ability to stop a former employee from using information in a competitive manner.

The GTSA was adopted before the proliferation of laptop computers, personal digital assistants, smart phones and other mobile electronic devices. Whereas proving a GTSA claim was once fairly straightforward, it has become more complicated with the advent of BlackBerrys®, iPhones™, cellular telephones and laptop computers. In the past, businesses primarily kept track of sensitive customer information – customers’ names, addresses, phone numbers, and preferences – in paper files. Now, contact information is most often stored electronically. Businesses

commonly keep customers’ names and contact information in a number of electronic formats and in multiple places. As a result, it is more difficult than ever to know who owns the information, and whether a business has made reasonable efforts to preserve its secrecy.

This article explains how the elements of the GTSA apply in the age of the BlackBerry® and iPhone™, and suggests some steps that company owners or executives can take right now to protect their trade secrets and preserve their rights under the GTSA.²

Showing It Belongs to FirstCo

To invoke the protection of the GTSA, FirstCo must first meet its most basic requirement: the information FirstCo is seeking to protect must belong to FirstCo. But, not all information is capable of being owned. Georgia courts have consistently ruled that a company can own tangible compilations of its customer contact information, but that it cannot own its customers’ names, email addresses or phone numbers alone. *See, e.g., Avnet, Inc. v. Wyle Labs*, 263 Ga. 615, 620, 437 S.E.2d 302, 305 (1993) (“tangible items” such as “handwritten, typed, printed or written information” would constitute “elements of an employer’s property so as to

SEE **BLACKBERRY**, Page 5

Labor & Employment Law Section Board of Directors 2009-2010

Chair

Robert W. Capobianco

Vice Chair/Chair-Elect

Mary M. (Peggy) Brockington

Secretary/Treasurer

Daniel M. Klein

Immediate Past Chair

Maureen Hernandez Sutton

Members at Large

Marcia A. Ganz

William C. (Cory) Barker

Lisa Chang

Julie S. Northup

E. Penn Payne

Debra Schwartz

Michelle E. Shivers

Michael Sullivan

James M. (Jim) Walters

Contact the Labor & Employment Law Section
Board of Directors at
sections@atlantabar.org

BLACKBERRY, continued from Page 4

be ‘lists’ of customers within the definition of ‘trade secrets’”) (citation omitted); *id.* at 618 (“[C]ustomers are not trade secrets.”) (emphasis in original) (citation omitted); see O.C.G.A. § 10-1-761(4); *Stone v. Williams General Corporation*, 266 Ga.App. 608, 612, 597 S.E.2d 456 (2004).

In the hypothetical scenario of FirstCo, this means that Sally – if not bound by a nondisclosure agreement or other restrictive covenant, would be free to solicit FirstCo’s customers so long as she relied on her own memory and/or publicly-available sources to recall those customers’ identities and contact information. It was only if Sally takes or copies an actual list contained on paper that the GTSA could stop her.

In the past, this tangible-intangible distinction provided an easy way to distinguish between compilations of names and the names themselves. But modern businesses seldom restrict their customers’ information to a single printed sheet of paper. Chances are, FirstCo keeps its customers’ contact information on a computer network or web-accessible database. In fact, FirstCo may keep this information in a number of formats: perhaps in an Excel spreadsheet for sales projections, in QuickBooks for billing and financial management purposes, and in Microsoft Outlook for communication needs. Perhaps the Outlook contact information syncs to employees’ BlackBerrys® or iPhones™. For a company like FirstCo, operating in an age of electronically stored information, how does the tangible-intangible distinction work?

So far, Georgia courts have offered little guidance. The most recent cases evaluating this issue have continued to find that businesses must put information in a tangible list in order for the information to be protected as a trade secret. In the 1997 case of *AmeriGas Propane, L.P. v. T-Bo Propane, Inc.*, 972 F.Supp. 685, the United States District Court for the Southern District of Georgia reaffirmed the tangible-intangible distinction as the trade secret threshold. The court declared, “companies may create customer lists on notebook paper, parchment, computer disk, microfiche, or on the back of a napkin; such tangible lists are protected by the [GTSA].” *Id.* at 698. The United States District Court for the Middle District of Georgia expressed the same view in *Hercules Automotive Products, Inc. v. Wedgestone Financial*, 245 B.R. 903 (M.D.Ga. 1999), when it rejected a company’s argument that former employees had stolen its “customer base.” The court chastised the company for being unable to point to a particular compilation of customer information that it alleged was stolen, telling the company that it “should have reduced its customer list to tangible, written form.”

Showing FirstCo Has Kept it a Secret

FirstCo must also show that it used reasonable efforts to maintain the secrecy of the information in question. O.C.G.A. § 10-1-761(4); see *Bacon v. Volvo Service Center, Inc.*, 266 Ga.App. 543, 544, 597 S.E.2d 440 (2004). It is not enough simply to declare that information is confidential; FirstCo must demonstrate that the company has taken affirmative actions to maintain the information’s secrecy. See *AmeriGas Propane v. T-Bo Propane, Inc.*, 972 F.Supp. 685, 701 (S.D.Ga. 1997) (questioning the legitimacy of the employer’s purported efforts to maintain the

secrecy of its customer lists where the lists “freely floated around the office without any system in place to track or monitor the whereabouts of the lists”).

In the past, a company could satisfy this requirement by showing that it maintained only one copy of its customer list, on paper, locked in a safe or a drawer that only executive management could access. See, e.g., *Stone v. Williams General Corp.*, 266 Ga.App. 608, 609, 611, 597 S.E.2d 456 (2004) (where a chemical company kept its customer list on a password-protected computer inside a locked room to which salespersons had no access, and prohibited sales representatives from taking customer information sheets home with them, the company had made reasonable efforts to keep its information secret). But, what qualifies as a “reasonable effort” to maintain secrecy if the information is stored in multiple electronic files rather than on paper?

Tax preparer H&R Block confronted this issue recently when it argued that its customer database was its trade secret. In *Paramount Tax & Accounting, LLC v. H&R Block Eastern Enterprises, Inc.*, 299 Ga. App. 596, 683 S.E.2d 141 (2009), a former H&R Block employee had used the database to send letters on behalf of a new tax preparer, soliciting H&R Block’s customers. The Court of Appeals recognized that H&R Block had established companywide policies protecting its client information from disclosure to third parties, counseled its employees regarding those policies, limited access to its customer database to certain employees, protected the database with a password, prohibited employees from printing out information from the database, and prohibited employees from taking the information home with them. Based on these confidentiality measures, the court decided that H&R Block had made a reasonable effort to protect the secrecy of its customer database.

H&R Block demonstrates the importance of instituting policies that restrict how employees may access and use information. See also *CMAX/Cleveland, Inc. v. UCR, Inc.*, 804 F.Supp. 337, 357 (M.D.Ga. 1992) (finding that a company had taken reasonable efforts to protect the secrecy of its software by placing

SEE **BLACKBERRY**, Page 6

Employment Law Review

Wednesday, March 24, 2010
at the State Bar of Georgia

To help prepare future volunteers for labor and employment-related pro bono opportunities, the employment law seminar covers general employment laws affecting non-profit organizations. Topics also include guidance on the creation or review of employee handbooks, proper compensation of employees and volunteers under the Fair Labor Standards Act and classification of workers as either independent contractors or employees.

Register online at www.atlantabar.org

BLACBERRY, continued from Page 5

proprietary notices on the software, requiring employees to sign confidentiality agreements, informing employees that the software was considered secret, and requiring employees whose work necessitated printing the software's source code to shred the printouts when they were finished with their work).

What Companies Such as FirstCo Can Do to Protect Their Information and Relationships

As the cases cited above show, there is little certainty for companies seeking to claim trade secret protection for their electronic lists and information. But there are some things companies can do now to avoid later problems:

1. *Require new employees to sign restrictive covenants.* Valid, enforceable restrictive covenants are the best way to prevent employees from using information acquired during their employment in the context of a new job. Companies should have their attorneys prepare an enforceable non-disclosure, non-compete and/or non-solicit agreement, and require all employees to sign it.
2. *Adopt confidentiality and computer use policies.* Companies should institute confidentiality, non-disclosure and computer use policies. A computer use policy should state that if an employee has a company-issued laptop computer or other electronic device, the employee must return it and may not download any information off of it before departing. Companies should disseminate their policies, train employees on what they mean, and enforce them.
3. *Issue company-owned laptops and BlackBerrys®.* Companies should issue company-owned laptops and BlackBerrys® to employees who need them to accomplish their work. Company executives should prohibit employees from accessing or downloading sensitive company information using personal computers or personally owned handheld devices so that if the company ever needs to assert its rights under the GTSA, it can show it attempted to maintain the secrecy of the information and that employees who downloaded that information knew they were exceeding their permission.
4. *Password-protect sensitive information.* Companies should password-protect databases, documents or other electronically stored information that contains sensitive information, and retain control of the password. Passwords should be changed often. To the extent that companies have hard copies of the information, these copies should be locked up, and access should be restricted.
5. *Restrict access.* Companies should permit access to sensitive information to only those employees who need it. Only those employees who need to access protected information should receive passwords, and those employees should be prohibited from distributing or disclosing the passwords.
6. *Label sensitive documents.* Sensitive documents, including customer lists, should be labeled "confidential" or "secret." Electronic documents should likewise be labeled or placed

in folders or drives that require a password to open.

7. *Destroy printed versions of sensitive documents.* Employees who print schedules and lists as part of their duties should be required to shred or otherwise destroy the lists when finished.
8. *Keep documents in the office.* Employees should be prohibited from taking sensitive documents home with them. Employees' access to customers' contact information or other sensitive information via their personal cell phones, BlackBerrys® or laptops should likewise be limited. Employee syncing of company computers with personal devices should be limited, and companies should implement strict policies concerning ownership in conjunction with any syncing that is permitted.
9. *Conduct inventory for departing employees.* Consistent with a computer use policy, departing employees should be required to return all company property, including documents and electronic devices issued through the company, and to delete any customer contact information that may be on their personal electronic devices.
10. *Institute remote access policies.* It is common for companies to provide remote access to work systems for employees who telecommute or are frequently out of the office. When companies know their employees need to access company information remotely, it is important to have in place policies that address the downloading of documents and other information. Employers may also want to consider limiting the scope of remote access.
11. *Act quickly.* If a key employee leaves and the company suspects he or she has taken information that could be a trade secret, consult with legal counsel immediately. The company may be able to seek the court's assistance to prevent its former employee from using its trade secrets.

*Benjamin I. Fink is a shareholder in Berman Fink Van Horn, P.C. Ben concentrates his litigation practice on disputes involving non-compete agreements, trade secrets and other competition-related claims.

Anne E. Andrews is an associate at Berman Fink Van Horn, P.C. Anne's practice involves a variety of business-related matters and focuses on the legal challenges facing nonprofit organizations and social enterprises.

(Endnotes)

1 Some protection may also be available under Georgia's Computer Systems Protection Act (the "Computer Protection Act") and similar statutes. A discussion of the Computer Protection Act is outside the scope of this article.

2 This article discusses the two elements of a GTSA claim that are most affected by the proliferation of BlackBerrys and similar devices: whether the information is owned by the company claiming trade secret protection, and whether the company used reasonable efforts to maintain the secrecy of the information. The remaining two elements – whether the information is commonly known by the public and whether it has economic value – are less affected by these recent technological developments, and are thus outside the scope of this article.