

IN THE UNITED STATES DISTRICT COURT
NORTHERN DISTRICT OF TEXAS
DALLAS DIVISION

**AFFILIATED COMPUTER SERVICES,
INC.**

Plaintiff,

v.

DUNCAN SOLUTIONS, INC.

Defendant.

§
§
§
§
§
§
§
§
§
§

CIVIL ACTION NO. _____

**ORIGINAL COMPLAINT AND APPLICATION FOR PRELIMINARY AND
PERMANENT INJUNCTION**

Plaintiff Affiliated Computer Services, Inc. (“ACS”) files this Original Complaint and Application for Preliminary Injunction, and Permanent Injunction. In support thereof, Plaintiff respectfully shows as follows:

I. INTRODUCTION

ACS recently made the shocking discovery that its direct competitor, Duncan Solutions, Inc., has established bogus Duncan email addresses in the name of at least twenty-five of ACS’s current employees, and these unauthorized email addresses are being used to divert ACS emails to Duncan’s computer network. To the average user, the email accounts for these ACS employees look like any normal email account for an ACS employee, with Microsoft Outlook displaying the person’s name (and not the complete email address) when such persons send or receive internal emails. In fact, without the consent of ACS or its employees, Duncan has injected unauthorized email accounts into email threads between ACS and Duncan, which has in turn cached Duncan emails in ACS’s system, so that emails sent to ACS employees are first forwarded to a Duncan email address in the ACS employee’s name, before being forwarded back

to the correct email address for the ACS employee. Duncan's unauthorized diversion of ACS's email not only interferes with the operation of ACS's computer network, but it also gives Duncan access to ACS's confidential and proprietary information and trade secrets – information that is frequently communicated via email at an information technology company such as ACS.

ACS seeks immediate injunctive relief to force Duncan to stop interfering with ACS's computer network. ACS is specifically entitled to such injunctive relief under the federal Computer Fraud and Abuse Act and two other federal statutes. Further, injunctive relief is also appropriate under the general standards applicable to granting a permanent injunction and a preliminary injunction. Indeed, there is simply no justification for allowing Duncan's unauthorized interference with its direct competitor's computer network, thus putting ACS's confidential and proprietary information and trade secrets at risk of disclosure. ACS therefore requests that the Court enter a temporary restraining order against Duncan, and that the Court grant ACS expedited discovery and other related relief.¹

II. PARTIES

1. Plaintiff Affiliated Computer Services, Inc. ("ACS") is a corporation organized under the laws of Delaware, with its principal place of business in Dallas, Texas.

2. Upon information and belief, Defendant Duncan Solutions, Inc. is a California corporation with its principal place of business located in Milwaukee, Wisconsin. Duncan Solutions, Inc. may be served through its registered agent in the State of California, Melissa Ward, 28 Hammond, Ste. C, Irvine, California 92618.

¹ ACS intends to file a Motion for Expedited Discovery, requesting expedited discovery and the opportunity to make a forensic image of Duncan's computers and servers for the purpose of capturing the extent of Duncan's digital subterfuge before those records are lost or manipulated.

III. JURISDICTION AND VENUE

3. This Court has subject matter jurisdiction over the lawsuit pursuant to the Computer Fraud and Abuse Act (18 U.S.C. § 1030), the Stored Wire and Electronic Communications and Transactional Records Access Act (18 U.S.C. § 2707), and the Federal Wiretapping Act (18 U.S.C. § 2520).

4. This Court also has subject matter jurisdiction over the lawsuit pursuant to 28 U.S.C. § 1332(a) because the parties are citizens of different States and the amount in controversy, exclusive of interest and costs, exceeds the sum of \$75,000.00.

5. Venue is proper in the Northern District of Texas and this Court pursuant to 28 U.S.C. § 1391(b)(2) because a substantial part of the events or omissions giving rise to the claims occurred in this judicial district. Duncan improperly accessed ACS's computer servers, which are located at its headquarters in Dallas, Texas, in order to re-route ACS's internal email to Duncan.

IV. FACTUAL BACKGROUND

A. ACS and Duncan are Direct Competitors.

6. ACS is a premier provider of diversified business process outsourcing and information technology services to commercial and government clients worldwide. ACS's offerings include business process outsourcing, information technology outsourcing, and systems and integration services. ACS's transportation business helps transportation agencies address such challenges as revenue collection and regulation compliance services worldwide. *See* Plaintiff's Appendix in Support ("App."), at Declaration of Jason Lyons, App. 001, ¶ 3; *id.* at Declaration of Mark Talbot, App. 015, ¶ 3.

7. ACS's global reach extends from its headquarters in Dallas, Texas, and across North America, Europe, the Middle East, Africa, the Caribbean, Latin America, and Asia Pacific. ACS's transportation business services clients in at least twenty-eight states in the United States,

and thirty countries around the world. ACS's computer network connects its offices, and facilitates ACS's electronic communication with its clients throughout the world. *See* App. 015, ¶ 4.

8. Duncan is a direct competitor of ACS's transportation business. *See* App. 015, ¶ 3². Duncan focuses on the parking and enforcement industry, offering its business solutions to municipalities, educational facilities, and other facilities. Duncan touts itself as the largest company in the parking and enforcement industry, claiming that it facilitates more than three billion parking and enforcement transactions.

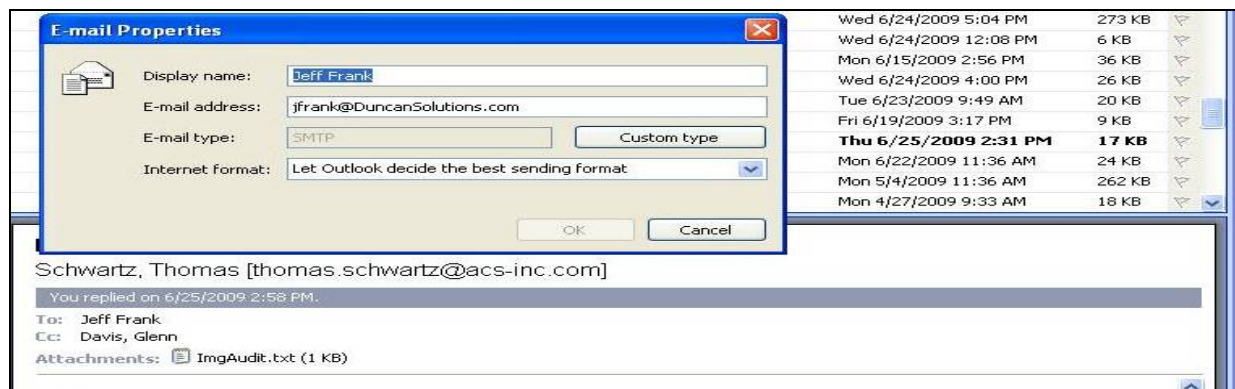
B. ACS Discovers an Unauthorized Duncan Email Address for an ACS Employee.

9. ACS uses Microsoft Outlook as its email application. For internal emails, ACS uses Outlook's default setting for displaying the names of employees that send and receive emails. Under that default setting, in the "To," "From," or "CC" fields in Microsoft Outlook, ACS employees would appear simply by their first and last name, instead of by such employees' complete email address. Thus, a hypothetical employee named John Smith would appear in the heading of an internal ACS email as John Smith, instead of as john.smith@acs-inc.com. *See* App. 001, ¶ 4.

10. In late June of this year, ACS employee Jeff Frank was exchanging emails with two fellow ACS employees, when he noticed a shocking and unauthorized change in his email address. Frank's real email address at ACS is jeff.frank@acs-inc.com. Yet, when Frank hit "Reply All" to send an email to his ACS colleagues, the display name continued to be the default setting of "Jeff Frank," but the email address in the "E-mail Properties" section of Outlook was shown as jfrank@DuncanSolutions.com. *See* App. 001, ¶ 5; App. 013 (Declaration of Jeff Frank), ¶ 3. Had

² Duncan's intense competitive nature is exemplified by its reaction to losing to ACS on the contract for monitoring and billing for parking meters in the City of Dallas. After losing, Duncan retaliated by sending the City of Dallas a broad FOIA request that included all documents relating to the implementation of the contract. A temporary injunction currently prohibits the City of Dallas from complying with Duncan's request.

Frank not fortuitously reviewed additional details about his email, he never would have discovered the problem. The screen view from Frank's computer is inserted below:



11. On the surface, the June email looked like a normal ACS internal email, with Frank's name displayed merely as "Jeff Frank." *See* App. 001, ¶ 5; App. 004. In reality, however, this email surreptitiously was routed to an email address at Duncan, and then was forwarded from Duncan back to Frank's ACS email address, with no perceptible delay in delivery. *See* App. 001-002, ¶ 6; App. 005-006. Thus, the average email user would have no idea that Duncan was secretly diverting email to its own network.

12. Because of this deception, the June email unwittingly transmitted an ACS internal audit report to Duncan. The internal audit report was never intended to be sent to ACS's direct competitor. *See* App. 014 (Declaration of Thomas Schwartz), ¶ 3.

C. ACS Conducts a Forensic Investigation.

13. Frank reported the issue to his supervisor, which triggered an investigation by ACS's Digital Forensic Group. *See* App. 001-002, ¶ 6. ACS conducted a forensic examination of the email accounts of three ACS employees, David Shive, Thomas Schwartz, and Jeff Frank, which revealed that their names in ACS's Microsoft Outlook are associated with the email addresses dshive@DuncanSolutions.com, tschwartz@DuncanSolutions.com, and jfrank@DuncanSolutions.com, respectively. *See* App. 002, ¶ 9. The investigation confirmed that (a) these ACS employees had

no knowledge that they have a Duncan email address, and (b) the Duncan email addresses were automatically forwarding emails to their valid ACS employee email accounts, david.shive@acs-inc.com, thomas.schwartz@acs-inc.com, and jeff.frank@acs-inc.com, respectively. ACS has also conducted tests that determined that the illegitimate Duncan email accounts remain active. *Id.*

14. ACS has conducted tests to determine how Duncan has interfered with ACS's computer network with this unauthorized email rerouting. The investigation has confirmed that when Duncan employees email ACS employees, Duncan's duplicative email addresses for ACS employees are being substituted for the correct emails in ACS's Microsoft Outlook address cache when anyone involved in the original email presses "Reply to All." *See, e.g.,* App. 009-012. In other words, when a Duncan employee emails an ACS employee, first the email is sent to the @duncansolutions.com address for the ACS employee, before being forwarded to the proper @acs-inc.com address, without any overt signs of its diversion to a duplicative Duncan email account. When anyone involved in that original email then presses "Reply to All," ACS's Outlook recognizes the first email address associated with the ACS employee name, which is the unauthorized @duncansolutions.com address, not the correct @acs-inc.com address. The problem then spreads when new ACS employees exchange emails with affected ACS employees, because the new employees inevitably will cache (or save) the ACS employee name associated with the unauthorized Duncan email address. Thus, once Duncan injects a Duncan email address into ACS's Outlook system, the unauthorized email address spreads virally. *See* App. 002, ¶ 10.

15. ACS has identified twenty-five employees that appear to have unauthorized Duncan email addresses set up under their names. *See* App. 002, ¶ 7; App. 008. Significantly, even though ACS's transportation business is a relatively small part of ACS's overall business, all twenty-five affected employees work in the transportation business that competes directly with Duncan. App. 015 at ¶ 5. Moreover, several of these employees hold high-level positions in

which they regularly review confidential and proprietary business information and trade secrets of ACS, as well as confidential and proprietary information that ACS receives from its clients. For example, the employees include four of the six regional managers for ACS's transportation business, and these regional managers have access to highly confidential information. *Id.*

D. ACS Takes Reasonable Steps to Protect Confidential and Trade Secret Information Sent or Received Via Email.

16. ACS takes very seriously its duty to protect the confidential and proprietary information that it generates internally and that ACS's clients provide to it. ACS distributes a written Information Security Standard manual to all employees, which details, in part, how to handle electronic confidential information. In accordance with that policy, confidential information, including sent and received email, is protected utilizing a hardened server, which is maintained within a secure environment at ACS's headquarters in Dallas, Texas. All ACS laptops are encrypted using advanced encryption techniques. All workstations are similarly encrypted where technically feasible; when technical or operational limitations prevent such encryption, step-by-step mitigating controls must be followed and documented to protect the electronic confidential information at that workstation. *See* App. 002, ¶ 12; App. 016, ¶ 7.

17. As an information technology company, ACS employees frequently send confidential and proprietary business information and trade secrets of ACS via email. For example, ACS employees regularly send and receive the following categories of protected information that would not be disclosed outside of the company: project proposals, client lists (including contact information that is not publicly available), internal financial reports, confidential client information, internal audit reports, business plans, and many other types of protected information. *See* App. 016, ¶ 6.

E. ACS Needs Immediate Injunctive Relief to Address Duncan's Actions.

18. While ACS has searched for a way to counter Duncan's access and diversion of company emails, ACS has not found an acceptable solution. For example, ACS could stop Duncan's duplicative routing of emails by blocking all emails from Duncan employees, but that would also prevent ACS from communicating with Duncan via email on the projects for which they have joint clients. *See App. 002, ¶ 11.*

19. ACS continues to investigate the nature and the scope of Duncan's unauthorized diversion of ACS emails. Because of the size limitations ACS imposes on individual employee mailboxes on the Microsoft Exchange server located at the Dallas headquarters, ACS must restore the back-up tapes stored in its Tarrytown, New York office. ACS has not yet been able to retrieve and search all back-up tapes that potentially may reveal additional employee emails or confidential information contained therein that has been unlawfully diverted by Duncan. ACS nonetheless has discovered an unauthorized Duncan email address that dates back to July 2007, thus raising serious concerns about the scope of Duncan's unauthorized email addresses and access of ACS's computers. *See App. 002, ¶ 13.*

20. Despite the egregious nature of Duncan's conduct, ACS will not be able to quantify effectively the vast majority of the harm it has suffered. Indeed, Duncan has gained a wholly improper competitive advantage by having the opportunity to review ACS's internal emails. The stolen emails reveal not only information about specific prospective and existing clients, but also confidential and proprietary information regarding ACS's general business strategies and plans; connecting this stream of communication to a specific lost business opportunity will be virtually impossible. Duncan's actions also interfere with ACS's operation of its daily business, because ACS is an information technology company that depends heavily

on the ability to communicate sensitive information via internal email. Monetary damages therefore clearly are an inadequate remedy. *See* App. 016, ¶ 8.

V. CAUSES OF ACTION

First Cause of Action: Computer Fraud and Abuse Act

21. ACS incorporates the preceding paragraphs as if fully set forth herein.
22. Pursuant to 18 U.S.C. § 1030, Duncan is knowingly or intentionally causing damage and loss to ACS by accessing ACS's protected computers without authorization.
23. Duncan has knowingly caused the transmission of a program, information, code or command that has modified ACS's internal email settings without the authorization of ACS or its clients, and further has intentionally accessed ACS's protected computer network without the authorization of ACS or any of its employees. Specifically, Duncan has manipulated and exploited ACS's Microsoft Outlook's address cache by associating ACS employee names with Duncan email addresses, knowing that the Outlook display names for the affected employees remain in the same format as for unaffected employees. Duncan has further hidden this substitution by double-routing emails intended for ACS employees, first delivering the emails to Duncan email accounts before then sending the same messages to proper ACS email accounts, so that the intended recipients are unaware, by looking at their names in the "To" lines of the emails, that their messages have been diverted to Duncan.
24. Furthermore, and in the alternative, Duncan has intentionally accessed ACS's protected computer network without authorization, through the above-described actions, and as a result of such conduct, has knowingly or recklessly caused damage and loss to ACS.
25. Duncan's actions have damaged ACS and its computer network, because Duncan's actions have allowed it to gain an unfair competitive advantage; have allowed Duncan to access confidential and proprietary information of ACS and its clients; have forced ACS to

incur the time and expense of a forensic investigation to determine the nature and extent of Duncan's conduct; and have interfered with and manipulated the internal settings on ACS's computer network. Duncan either knowingly caused such damages, or it acted recklessly in causing such damages.

26. Within a period of one year or less, Duncan's actions have caused ACS to incur damages of substantially more than the statutory requirement of \$5,000. ACS is also entitled to recover its reasonable and necessary attorneys' fees.

Second Cause of Action: Wiretap Act

27. ACS incorporates the preceding paragraphs as if fully set forth herein.

28. Pursuant to 18 U.S.C. § 2511, Duncan has intentionally intercepted ACS's electronic communications by modifying ACS's internal email settings without the authorization of ACS or its clients, and by intentionally accessing ACS's protected computer network without the authorization of ACS or any of its employees.

29. ACS's email communications rely on devices that are affixed to or otherwise transmit a signal through a wire, cable, or other like connection used in wire communications. Moreover, ACS's email communications took place at its headquarters in Dallas, where ACS is regularly engaged in interstate and foreign commerce. The information illegally obtained by Duncan also relates to ACS's operations in interstate and foreign commerce.

30. Pursuant to 18 U.S.C. §2520, ACS is entitled to recover civil damages for Duncan's violations. As a result of Duncan's actions, ACS has suffered actual damages in an amount to be proved at trial. In addition, ACS is entitled to recover statutory damages of the greater of \$100 a day for each day of Duncan's violations, or \$10,000, as well as its reasonable and necessary attorneys' fees.

Third Cause of Action: Stored Communications Act

31. ACS incorporates the preceding paragraphs as if fully set forth herein.

32. Under 18 U.S.C. § 2701, Duncan has intentionally accessed the facilities for ACS's computer network, which ACS uses to provide electronic communications services for the company. Upon gaining such access, Duncan has unlawfully modified ACS's internal email settings without the authorization of ACS or its clients, and has intentionally accessed ACS's protected computer network without the authorization of ACS or any of its employees.

33. Upon accessing ACS's facilities without authorization, Duncan obtained, altered, or prevented authorized access to ACS's stored email communications by illegally routing emails stored on ACS's computer network to its own computer network.

34. ACS has a civil cause of action against Duncan under 18 U.S.C. § 2707. As a result of Duncan's actions, ACS has suffered actual damages in an amount to be proved at trial. ACS is also entitled to recover its reasonable attorneys' fees and other litigation costs reasonably incurred.

Fourth Cause of Action: Texas Harmful Access By Computer Act

35. ACS incorporates the preceding paragraphs as if fully set forth herein.

36. Duncan knowingly or intentionally accessed ACS's computers, computer network, and/or computer system without the effective consent of ACS, the owner of those computers.

37. Duncan knowingly or intentionally obtained a benefit, harmed ACS, and/or altered, damaged, or deleted ACS's property through this unauthorized access.

38. The aggregate amount involved in this unauthorized access of ACS's computers is at least \$20,000.

Fifth Cause of Action: Misappropriation of Trade Secrets

39. ACS incorporates the preceding paragraphs as if fully set forth herein.

40. As an information technology company, ACS employees frequently send confidential and proprietary business information and trade secrets of ACS via email. For example, ACS employees regularly send and receive the following categories of protected information that would not be disclosed outside of the company: project proposals, client lists (including contact information that is not publicly available), internal financial reports, confidential client information, internal audit reports, business plans, and many other types of protection information. The foregoing information constitutes trade secrets, as that term is defined under Texas law.

41. Duncan has created unauthorized Duncan email addresses for numerous ACS employees who have access to the protected information of ACS and its clients. Because Duncan is secretly diverting ACS emails to its own computer network, Duncan has direct access to ACS's protected information that is regularly communicated via email.

42. Duncan's access to ACS's protected information has never been authorized by ACS or any of its employees. Duncan has gained such access despite ACS's substantial precautions to protect confidential and proprietary information and trade secrets from disclosure.

43. Upon information and belief, Duncan is using ACS's confidential information to gain an unfair competitive advantage.

44. Duncan's actions are a proximate cause of the damages for which ACS now sues. These damages are ongoing and will continue to damage ACS in an amount within the jurisdictional limits of this Court.

45. As a direct and proximate result of Duncan's intentional conduct, ACS has suffered damages in an amount to be proven at trial.

Sixth Cause of Action: Request for Preliminary Injunction.

46. ACS incorporates the preceding paragraphs as if fully set forth herein.

47. The affidavits of Jason Lyons, Jeff Frank, Thomas Schwartz, and Mark Talbot are contained in Plaintiff's Appendix in Support hereof. These affidavits prove the allegations in this application for injunctive relief.

48. Duncan has created unauthorized Duncan email addresses for ACS employees, and Duncan has interfered with and harmed ACS's computer network by diverting ACS's internal email to Duncan's computer network. Further, Duncan has attempted to conceal its activities, interfering with ACS's normal internal settings so that there is no indication to the average user that they have a fake Duncan email address or that Duncan is diverting their email without authorization.

49. ACS is entitled to injunctive relief because it has established a likelihood of success on its claim against Duncan for violations of the Computer Fraud and Abuse Act, which specifically provides for injunctive relief. For this reason alone, ACS is entitled to a preliminary injunction.

50. Duncan's actions also violate the federal wiretapping act, which also entitles ACS to injunctive relief to stop Duncan's unlawful conduct. *See* 18 U.S.C. § 2520(b)(1). Similarly, Duncan's violation of the Stored Communications Act gives ACS the right to obtain injunctive relief. *See* 18 U.S.C. § 2707(b)(1).

51. In addition, ACS has been and will continue to suffer immediate and irreparable damage if Duncan is not enjoined during the pendency of this lawsuit from interfering with ACS's computer network; from using the wholly unauthorized Duncan email addresses that it has established for ACS employees; and from accessing current and future ACS emails that are not intended for distribution to a competitor and that contain confidential and proprietary

information and trade secrets of ACS or its clients. ACS needs the Court's assistance in addressing Duncan's illegal actions, because ACS cannot block all email communications from Duncan's computer network due to the situations in which ACS and Duncan must work together to serve mutual clients. Moreover, ACS will not be able to quantify effectively the vast majority of the harm it has suffered. Indeed, Duncan has gained a wholly improper competitive advantage by having the opportunity to review ACS's internal emails, but it will be impossible in most instances for ACS to connect the stolen emails to a specific lost business opportunity. Duncan's actions also interfere with ACS's operation of its daily business, because ACS is an information technology company that depends heavily on the ability to communicate sensitive information via internal email. Monetary damages therefore clearly are an inadequate remedy.

52. There is a substantial likelihood that ACS will prevail on the merits of the claims that it has alleged in this lawsuit. Indeed, the evidence submitted in connection with this request establishes that Duncan has engaged in conduct raising a strong inference that Duncan has intentionally interfered with ACS's computer network and diverted ACS emails.

53. Any potential harm associated with the entry of a preliminary injunction is outweighed by the potential damage to ACS's internal business operations and the threat to ACS's confidential and proprietary information and trade secrets. Indeed, there is simply no legitimate justification with Duncan's interference with ACS's computer network and internal business operations.

54. Issuance of a preliminary injunction would not adversely affect the public interest and public policy because the public interest is served by preventing companies from interfering with their competitors' computer networks.

55. The Court should enter a preliminary injunction because ACS will suffer immediate and irreparable injury, loss, or damage if the preliminary injunction is not granted. Moreover, there is no less drastic means to protect ACS's interests.

56. ACS further asks this Court to set its application for preliminary injunction for hearing at the earliest possible time. After the hearing, ACS requests that the Court issue a preliminary injunction against Duncan prohibiting Duncan from interfering with ACS's computer network; from using the wholly unauthorized Duncan email addresses that it has established for ACS employees; and from accessing current and future ACS emails that are not intended for distribution to a competitor and that contain confidential and proprietary information and trade secrets of ACS or its clients.

57. ACS is willing to post a bond in the amount that the Court deems appropriate.

Seventh Cause of Action: Request for Permanent Injunction

58. ACS incorporates the preceding paragraphs as if fully set forth herein.

59. ACS further ask the Court to set its application for injunctive relief for a full trial on the issues in this application, and, after the trial, to issue a permanent injunction against Duncan from interfering with ACS's computer network; from using the wholly unauthorized Duncan email addresses that it has established for ACS employees; and from accessing current and future ACS emails that are not intended for distribution to a competitor and that contain confidential and proprietary information and trade secrets of ACS or its clients.

VI. JURY DEMAND

60. ACS hereby demands resolution of these matters by Jury Trial.

VII. PRAYER

Plaintiff Affiliated Computer Services, Inc. asks this Court to enter judgment against Defendant Duncan Solutions, Inc. for the following relief:

1. All damages sustained as a result of Duncan Solutions' unauthorized access of ACS's computer network, with such quantifiable damages exceeding \$100,000;
2. Entry of a preliminary injunction, and permanent injunction, as requested herein;
3. Compensatory damages in an amount to be determined at trial;
4. Punitive damages in an amount to be determined at trial;
5. Reasonable and necessary attorney's fees in an amount to be determined at trial;
6. Prejudgment and post-judgment interest as provided by law; and
7. For all other relief as the Court deems appropriate, at law or in equity.

DATED: August 18, 2009

Respectfully submitted,

/s/ John T. Cox III

John T. Cox III

Texas Bar No. 24003722

Christopher J. Akin

Texas Bar No. 00793237

Renee S. Strickland

Texas Bar No. 24041983

LYNN TILLOTSON PINKER & COX, LLP

2100 Ross Avenue, Suite 2700

Dallas, Texas 75201

Phone (214) 981-3800

Fax (214) 981-3839

ATTORNEYS FOR PLAINTIFF