

**North Carolina Security Breach Reporting Form  
Pursuant to the Identity Theft Protection Act of 2005**

Name of Business Owning or Licensing Information Affected by the Breach:	<u>Administaff</u>	<b>PLEASE SUBMIT FORM TO:</b> Consumer Protection Division NC Attorney General's Office 9001 Mail Service Center Raleigh, NC 27699-9001 Telephone: (919) 716-6000 Toll Free in NC: (877) 566-7226 FAX: (919) 716-6050
Address:	<u>19001 Crescent Springs Drive Kingwood, TX 77339-3802</u>	
Telephone:	<u>(281) 312-3577</u>	
Fax:	<u>(281) 348-3908</u>	
Email:	<u>carl_curtis@administaff.com</u>	

Date Security Breach Reporting Form submitted: 10/15/07

Date the Security Breach was discovered: 10/03/07

Estimated number of affected individuals: 159,000

Estimated number of NC residents affected: 3,050

Name of business maintaining or possessing information that was the subject of the Security Breach, if the business that experienced the Security Breach is not the same entity as the business reporting the Security Breach (pursuant to N.C.G.S. § 75-65(b)): Administaff

Describe the circumstances surrounding the Security Breach and state whether the information breached was in electronic or paper format: Electronic. See attached Press Release.

Regarding electronic information breached, state whether the information breached or potentially breached was password protected or encrypted in some manner. Yes If so, please describe the security measures protecting the information: Password Protected with a sophisticated password in accordance with best practices for password level security.

Describe any measures taken to prevent a similar Security Breach from occurring in the future: See attached Administaff Information Technology Security document.

Date affected NC residents were/will be notified: Estimated to be approx. the week of 10/15/07.

If there has been any delay in notifying affected NC residents, describe the circumstances surrounding the delay pursuant to N.C.G.S. § 75-65(a) and (c): Not applicable.

If the delay was pursuant to a request from law enforcement pursuant to N.C.G.S. § 75-65(c), please include the written request or the contemporaneous memorandum.

How NC residents were/will be notified? (pursuant to N.C.G.S. § 75-65(e))

Please attach copy of the notice if in written form or a copy of any scripted notice if in telephonic form.

written notice  
 electronic notice (email)  
 telephone notice  
 substitute notice

Signature: Carl L. Curtis Date: 10/15/07

Contact Person, Title: Carl L. Curtis, Assistant General Counsel

Address: Same as above.

(if different from above)

Telephone: (281) 312-3577 Fax: (281) 348-3908 Email: carl\_curtis@administaff.com



---

**News Release*****Investor Relations Contact:***

Douglas S. Sharp  
Vice President of Finance,  
Chief Financial Officer and Treasurer  
(281) 348-3232  
[Douglas\\_S Sharp@Administaff.com](mailto:Douglas_S Sharp@Administaff.com)

***News Media Contact:***

Jason Cutbirth  
Managing Director of  
Marketing and Corporate Communications  
(281) 312-3085  
[Jason\\_Cutbirth@Administaff.com](mailto:Jason_Cutbirth@Administaff.com)

**ADMINISTAFF NOTIFIES CALENDAR YEAR 2006 WORKSITE  
EMPLOYEES OF MISSING LAPTOP COMPUTER CONTAINING  
PERSONAL INFORMATION**

HOUSTON – Oct. 15, 2007 – Administaff, Inc. (NYSE: ASF), a leading provider of human resources services for small and medium-sized businesses, today announced that a company laptop computer containing personal information about individuals who were Administaff worksite employees during calendar year 2006 has been reported missing.

The facts as determined by the company's investigation strongly indicate that this was a random event, and that the personal information was not specifically targeted. At this time, the company has no reason to believe that the personal information has been accessed or used improperly. The laptop computer, which was reported missing on Oct. 3, 2007, is password protected; however, the personal information was not saved in an encrypted location, which is a clear violation of company policies.

The confidential data was being compiled in response to a governmental reporting requirement and included names, addresses and Social Security numbers for most worksite employees paid by Administaff in 2006.

The company is taking steps to notify approximately 96,000 former worksite employees and approximately 63,000 current worksite employees in writing and will offer to them one year of free credit monitoring services with fraud resolution assistance. Administaff has also established a toll-free dedicated helpline and Web site for affected individuals and clients. Affected individuals can find additional information to assist them at <http://www.administaff.com/idprotection>.

(more)

Administaff, Inc.

Page 2

"Maintaining the integrity of confidential information is of utmost importance to Administaff, and we continue to take appropriate measures to safeguard the security of personal data," said Paul J. Sarvadi, Administaff chairman and chief executive officer. "We deeply regret that this incident occurred. While we have no evidence to suggest the information stored on the computer has been accessed or misused, we are taking precautionary measures to ensure that the affected individuals have resources available to protect themselves."

Administaff is the nation's leading professional employer organization (PEO), serving as a full-service human resources department that provides small and medium-sized businesses with administrative relief, big-company benefits, reduced liabilities and a systematic way to improve productivity. The company operates 47 sales offices in 23 major markets. For additional information, visit Administaff's Web site at <http://www.administaff.com>.

*The statements contained herein that are not historical facts are forward-looking statements within the meaning of the federal securities laws (Section 27A of the Securities Act of 1933 and Section 21E of the Securities Exchange Act of 1934). You can identify such forward-looking statements by the words "expects," "intends," "plans," "projects," "believes," "estimates," "likely," "possibly," "probably," "goal," "objective," "target," "assume," "outlook," "guidance," "predicts," "appears," "indicator" and similar expressions. Forward-looking statements involve a number of risks and uncertainties. In the normal course of business, Administaff, Inc., in an effort to help keep our stockholders and the public informed about our operations, may from time to time issue such forward-looking statements, either orally or in writing. Generally, these statements relate to business plans or strategies, projected or anticipated benefits or other consequences of such plans or strategies, or projections involving anticipated revenues, earnings, unit growth, profit per worksite employee, pricing, operating expenses or other aspects of operating results. We base the forward-looking statements on our current expectations, estimates and projections. These statements are not guarantees of future performance and involve risks and uncertainties that we cannot predict. In addition, we have based many of these forward-looking statements on assumptions about future events that may prove to be inaccurate. Therefore, the actual results of the future events described in such forward-looking statements could differ materially from those stated in such forward-looking statements. Among the factors that could cause actual results to differ materially are: (i) changes in general economic conditions; (ii) regulatory and tax developments and possible adverse application of various federal, state and local regulations, including but not limited to the California State Unemployment Tax matter; (iii) changes in our direct costs and operating expenses including, but not limited to, increases in health insurance costs and workers' compensation rates and underlying claims trends, financial solvency of workers' compensation carriers and other insurers, state unemployment tax rates, liabilities for employee and client actions or payroll-related claims, changes in the costs of expanding into new markets, and failure to manage growth of our operations; (iv) the effectiveness of our sales and marketing efforts; (v) changes in the competitive environment in the PEO industry, including the entrance of new competitors and our ability to renew or replace client companies; (vi) our liability for worksite employee payroll and benefits costs; and (vii) an adverse final judgment or settlement of claims against Administaff. These factors are discussed in further detail in Administaff's filings with the U.S. Securities and Exchange Commission. Any of these factors, or a combination of such factors, could materially affect the results of our operations and whether forward-looking statements we make ultimately prove to be accurate.*

###

# Administaff Information Technology Security

## *Executive Summary*

### Overview

Businesses are exposed to a range of security risks inherent with information technology systems. These risks have the potential to disrupt company operations, cause business failure or even disclose sensitive information. Proper management for these risks permits a company to anticipate vulnerabilities, develop technology policies, and deploy technology that will minimize the effects of a security risk.

Administaff takes information technology security seriously. We know that a security incident of our information systems will not only affect us, but our customers as well. Security Policies, Security and Awareness Training, enterprise level security infrastructure components, internal and external assessments, and independent audits are several methods we use to protect ourselves against a security event.

### Security Policy

Administaff is held accountable to a Technology Security Policy. This security framework, which encompasses over 27 policies, outlines the configuration, expected behavior, enforcement, exceptions etc. for security objects in our environment. Examples would include: Backup and Restoration Policy, Disposal of Electronic Media Policy, Corporate Software Policy, Change Management Policy, Intranet Policy, Monitoring Policy, Audit and Risk Assessment Policy, and Encryption Policy.

### Security and Awareness Training

Security education of the Administaff workforce is a priority. Our comprehensive security and awareness program is mandatory for all Administaff employees. We not only ensure that our technical staff is trained on the security of all our systems and applications, but we require that all of our employees go through our security training so they understand how to protect our assets and our client's information.

### Enterprise Security Infrastructure

Administaff has deployed several industry standard security products to help reduce risk. Since Administaff has an Internet presence, enterprise class firewalls, intrusion detection and prevention systems, virtual private networking switches, and managed anti-virus systems have been put in place. Vulnerability assessment scanners, malicious software scanners, security event management technology and Internet content filters among other tools, are in place to identify and protect our internal systems.

### Assessments and Auditing

According to our Audit and Risk Assessment Policy, Administaff periodically conducts assessments against deployed security controls. Administaff utilizes both internal and external parties for assessment of these security infrastructure components. Administaff employs a Computer Security Incident Response Team. This team is utilized for restoring and maintaining normal business continuity, increasing the defense and survivability against future incidents, and deterring future incidents by acts of assessments, investigation and prosecution.

With the introduction of the Sarbanes Oxley Act of 2002 and HIPAA Privacy and Security Acts, Administaff has setup auditing standards that are aligned with each of these compliance efforts. Yearly, Administaff conducts technology audits with an external auditing team to achieve our compliance goals. This comprehensive auditing is conducted against the Administaff Technology Security Policy, our technology infrastructure, and our business processes.



We take care of your people.  
So you can take care of your business®

Corporate Headquarters - Houston  
19001 Crescent Springs Drive  
Kingwood, Texas 77339-3802  
[www.administaff.com](http://www.administaff.com) 800-465-3800