

JAN 23 2008

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: SavaSeniorCare Administrative Services, LLC

Address: 1 Ravinia Drive, Suite 1500

Atlanta, Georgia 30346

Telephone: 678-443-6786

Fax: 678-443-6782

Email: smmiele@savasc.com

PLEASE SUBMIT FORM TO:

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

Date Security Breach Reporting Form Submitted: January 18, 2008

Date the Security Breach was discovered: January 4, 2008

Estimated number of affected individuals: 25,749

Estimated number of NC residents affected: 4,405

Name of the 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)): Windham Brannon, P.C.

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

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: The computer was password protected.

Describe any measures taken to prevent a similar Security Breach from occurring in the future: The Company is revising its policies and procedures regarding the dissemination of confidential data to outside parties.

Date affected NC residents were/will be notified: Beginning on January 18, 2008.

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): Investigation to determine scope of breach. See attached for details.

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: 

Date: January 18, 2008

Contact Person, Title: Stefano Miele, Executive Vice President, General Counsel

Address: Same as above

(if different from above) N/A

Telephone: 678-443-6786

Fax: 678-443-6782

Email: smmiele@savasc.com

# **ATTACHMENT A**

On the evening of December 31, 2007, the offices of Windham Brannon, P.C. ("Windham") in Atlanta, Georgia were burglarized and several laptop computers were stolen, as well as some amount of cash. Windham provides audit services for SavaSeniorCare Administrative Services, LLC's ("Sava") 401(k) benefit plan, and one of the stolen computers, which was password protected, contained unencrypted personal information about Sava employees and former employees eligible to participate in its 401(k) plan. Windham discovered the theft on January 2, 2008 and reported it to the Atlanta Police Department. Windham notified Sava of the incident on January 4.

The stolen computer that contained information about Sava employees and former employees was recovered by the Atlanta Police Department on January 7, 2008 and was returned to Windham on the following day. Through its counsel, Sava then engaged forensic computer examiners at Navigant Consulting to inspect the computer in an effort to determine whether any files containing personal information had been accessed. Windham made the laptop available to the examiners on January 9, and the examiners conducted their analysis on January 10 and 11. The examiners found that the computer was reformatted within a few hours of the theft and that, as a result, most of the files containing personal information about Sava employees and former employees had been destroyed. Consequently, the examiners were not able to determine with certainty whether these files were accessed before they were destroyed. The examiners did inspect the data files of other clients that survived the reformatting process and determined that none of these files were accessed at any time after the theft.

# **ATTACHMENT B**

January 18, 2008

**NOTICE OF SECURITY BREACH  
INVOLVING YOUR PERSONAL INFORMATION**

We are writing to inform you of a security breach involving your personal information.

We recently received notice that several laptop computers were stolen on December 31, 2007 from the offices of an accounting firm that provides audit services for our 401(k) benefit plan. One of these laptops contained sensitive information concerning our 401(k) plan, including your name, home address, social security number, and date of birth. This laptop also may have contained your salary, 401(k) account number, and 401(k) balance information. The password to access your 401(k) account was not contained on the laptop. Although the laptop was password protected, the information stored on it was not encrypted.

The theft was reported to local law enforcement officials, who recovered the laptop that contained your personal information on January 7, 2008. After the laptop was recovered, we engaged forensic computer examiners to determine if any files on the laptop had been accessed. In the course of their investigation, these examiners found that the laptop had been reformatted within hours of the theft and that, as a result, substantially all of the files containing your personal information were destroyed. The examiners also inspected files on the laptop that survived the reformatting process and determined that none of these files were accessed after the theft. Although we cannot be certain that files were not downloaded or copied before the laptop was reformatted, we have no evidence at this time indicating that your personal information has been misused, accessed, or retained by unauthorized persons.

Because there is some risk that your personal information has been compromised and could be misused, you should be vigilant for suspicious activity concerning your identity and financial and credit accounts. We have notified Fidelity, our 401(k) plan administrator, of this security breach, and Fidelity has informed us that, to date, no suspicious activity has been reported to Fidelity concerning our 401(k) plan. Nevertheless, we recommend that you access your 401(k) account and change your password immediately.

There are other steps that you can take to minimize any potential risk of identity theft. The Federal Trade Commission recommends, among other things, that you review your credit reports for unusual activity. Under federal law, you are entitled each year to one free copy of your credit report from the three national consumer credit reporting agencies. To request a copy of your credit report, visit <http://www.annualcreditreport.com>, call 1-877-322-8228, or write to Annual Credit

# Sava

---

Page 2  
January 18, 2008

Report Request Service, P.O. Box 105281, Atlanta, Georgia 30348-5281. You also should review your financial account and billing statements carefully for unusual activity.

If you detect suspicious activity, the Federal Trade Commission recommends that you contact one of the three national consumer credit reporting agencies and request that they place a "fraud alert" on your credit file. A fraud alert directs creditors to follow certain procedures before they open new accounts in your name or modify your existing accounts. You can contact the national consumer credit reporting agencies as follows:

|   |   |  |
|---|---|--|
| Equifax<br>(888) 766-0008<br><a href="http://www.equifax.com">http://www.equifax.com</a><br>P.O. Box 740241<br>Atlanta, GA 30374-0241 | Experian<br>(888) 397-3742<br><a href="http://www.experian.com">http://www.experian.com</a><br>P.O. Box 9532<br>Allen, TX 75013 | TransUnion<br>(800) 680-7289<br><a href="http://www.transunion.com">http://www.transunion.com</a><br>P.O. Box 6790<br>Fullerton, CA 92834-6790 |
|---|---|--|

In some states, you also may have a right to request a "credit freeze," which requires the use of a personal identification number issued to you at the time you request the freeze to open any new credit account. Procedures for requesting a credit freeze may vary from state to state, and there may be fees for placing, lifting, or removing a credit freeze. For more information, contact the national consumer credit reporting agencies.

Finally, if you have reason to believe that you are a victim of identity theft, you also should report the matter to appropriate law enforcement agencies, including the Federal Trade Commission, and to us.

For more information on steps that you can take to prevent and detect identity theft, visit the website of the Federal Trade Commission at <http://www.ftc.gov>.

If we subsequently learn that your personal information, in fact, was accessed by unauthorized persons, we will contact you and provide you with additional details. If you have any questions, we have set up a toll-free number for you to contact us at (866) 272 - 3118.

Sincerely,



L. Scott Bardowell  
Executive Vice President, Human Resources