

RECEIVED  
16 FEB -9 AM 10:15  
CONSUMER PROTECTION DIV.

**Vickie B. Ahlers**

1500 Woodmen Tower  
1700 Farnam St  
Omaha, NE 68102-2068  
Tel: 402.344.0500  
Fax: 402.344.0588  
Direct: 402.636.8230  
vahlers@bairdholm.com  
www.bairdholm.com  
Also admitted in Iowa

February 5, 2016

**CERTIFIED, RETURN RECEIPT REQUESTED**

Director, Consumer Protection Division  
Office of the Attorney General of Iowa  
Hoover State Office Building  
1305 E. Walnut Street  
Des Moines IA 50319

Re: Notification of Data Security Incident Involving Iowa Residents

Dear Sir/Madam:

This firm represents Seim Johnson, LLP ("Seim Johnson") located in Omaha, Nebraska. On behalf of Seim Johnson, we hereby submit this letter as notice of a recent data security incident, as required under Iowa Code § 715C.2.

Seim Johnson provides administrative services to health care providers. Administrative services can include auditing the provider's financial statements and assisting in the preparation of reports the provider is required to file with Medicare and/or Medicaid. In order to perform these services, Seim Johnson receives limited personal information of patients of the provider.

On December 15, 2015, Seim Johnson learned that a laptop computer belonging to one of its employees had been stolen from the employee's vehicle between December 11, 2015 and December 14, 2015, in the Nashville, Tennessee area. Personal information of certain individuals receiving services from some of Seim Johnson's health care provider clients across the Midwest may be affected, including two health care providers doing business in Iowa. Those providers are Lakes Regional Healthcare and Knoxville Hospital & Clinics. Approximately 10,000 Iowa residents may be affected. Seim Johnson is working with the health care providers impacted and this notice is being submitted on the providers' behalf as well.

Seim Johnson has a portable computer encryption policy and utilizes CheckPoint Whole Disk Encryption (WDE). WDE is installed and deployed on all Seim Johnson portable computers, including the stolen laptop computer. As part of Seim Johnson's initial investigation, Seim Johnson sought to verify its understanding that the stolen laptop computer was encrypted. Its understanding was based on "dashboard" confirmations of encryption produced by the software. Seim Johnson had relied on this confirmation in allowing laptop computers to be used by its employees while traveling. Despite getting this confirmation of encryption on the stolen laptop computer, through further investigation after the theft Seim Johnson discovered the encryption software likely was not functioning properly on the stolen laptop computer.

The information on the laptop computer may have included identifiers such as the individual's patient account number, medical record number or visit number with a name sometimes listed with that number. For a few individuals, other limited information such as

service dates, primary payer, account balance or department of service (for example, "ER") may also have been included. Social Security numbers were not included for any Iowa citizens, as well as the information did not include address or credit card information.

Attached is a copy of the letter Seim Johnson sent to all impacted individuals for whom the health care provider had valid addresses by U.S. Postal mail. The letters were post-marked on February 3, 2016. To reach individuals for whom no current address was available, a public notice also has been placed in the Des Moines Register with expected publication dates of February 8<sup>th</sup> – February 12<sup>th</sup>. The notification steps taken by Seim Johnson on behalf of the affected health care providers are in compliance with the Health Insurance Portability and Accountability Act of 1996 ("HIPAA").

To protect all individuals affected by this incident, including those citizens of Iowa, Seim Johnson has arranged to have AllClear ID protect the individual's identity for 12 months at no cost to the individual.

Seim Johnson takes its obligation to protect personal information very seriously. It is reviewing its security protocols and is adopting additional policies, procedures and training to ensure that all personal information is maintained securely.

Please direct any questions regarding this incident to the undersigned at the above address.

Sincerely,



Vickie B. Ahlers  
FOR THE FIRM

Enclosure

cc: Roger Thompson, Seim Johnson (w/encl.)  
DOCS/1599668.1



00001  
JOHN Q. SAMPLE  
1234 MAIN STREET  
ANYTOWN US 12345-6789

February 3, 2016

Dear John Sample,

We are writing to you about the possible loss of your personal information.

Seim Johnson is an accounting business that works with Client\_def1 ("Provider"). We audit the Provider's financial statements. We help the Provider prepare reports it must file with Medicare or Medicaid. When we work with the Provider, we receive some personal information about the Provider's patients. We may receive information about the services the Provider provided to you and its charges for those services.

On December 15, 2015, we learned that a laptop computer used by one of our employees was stolen from the employee's vehicle. This happened between December 11, 2015 and December 14, 2015 in Nashville, Tennessee. The laptop computer has not been found. When we learned what happened, we started an investigation. Seim Johnson's standard procedure to secure data on all of its laptop computers includes installing a password and encryption software. After the theft, we learned that it was likely that the encryption software on the stolen laptop computer was not functioning.

Information on the stolen laptop computer included a personal identifier such as your patient account number, medical record number or visit number with a name sometimes listed with that number. For a few individuals, other limited information such as address, service dates, primary payer, account balance or department of service (for example, "ER") may also have been included. The information did not include your Social Security number or credit card information.

We do not believe the laptop computer was stolen for its information. On behalf of Client\_def1, we must tell you about what happened. We must also tell you about steps you may take to prevent identity theft or fraud. Please review the enclosed Information about Identity Theft Protection.

As an added precaution, we have arranged to have AllClear ID protect your identity for 12 months at no cost to you. The following identity protection services start on the date of this notice and you can use them at any time during the next 12 months.



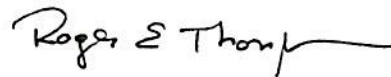
AllClear SECURE: The team at AllClear ID is ready and standing by if you need identity repair assistance. This service is automatically available to you with no enrollment required. If a problem arises, simply call 1-877-263-7997, provide your Reference Code Redemption Code, and a dedicated investigator will help recover financial losses, restore your credit and make sure your identity is returned to its proper condition.

The security of your information is very important. We are reviewing our security practices and taking steps to prevent a similar occurrence. We are training our employees on firm policies and procedures for protecting personal information.

We have set up a toll-free number for any questions you have. **The toll-free number is 1-877-263-7997.**

We are very sorry about any inconvenience or concerns because of this incident.

Sincerely,

A handwritten signature in black ink that reads "Roger E. Thompson". The signature is written in a cursive style with a long horizontal flourish at the end.

Roger Thompson, Managing Partner  
Seim Johnson LLP  
18081 Burt Street, Suite 200  
Omaha, NE 68022-4722

## **Information about Identity Theft Prevention**

We recommend that you regularly review statements from your accounts and periodically obtain your credit report from one or more of the national credit reporting companies. You may obtain a free copy of your credit report online at [www.annualcreditreport.com](http://www.annualcreditreport.com), by calling toll-free 1-877-322-8228, or by mailing an Annual Credit Report Request Form (available at [www.annualcreditreport.com](http://www.annualcreditreport.com)) to: Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA, 30348-5281. You may also purchase a copy of your credit report by contacting one or more of the three national credit reporting agencies listed below.

**Equifax:** P.O. Box 740241, Atlanta, Georgia 30374-0241, 1-800-685-1111, [www.equifax.com](http://www.equifax.com)  
**Experian:** P.O. Box 9532, Allen, TX 75013, 1-888-397-3742, [www.experian.com](http://www.experian.com)  
**TransUnion:** P.O. Box 1000, Chester, PA 19022, 1-800-888-4213, [www.transunion.com](http://www.transunion.com)

When you receive your credit reports, review them carefully. Look for accounts or creditor inquiries that you did not initiate or do not recognize. Look for information, such as home address and Social Security number, that is not accurate. If you see anything you do not understand, call the credit reporting agency at the telephone number on the report.

We recommend you remain vigilant with respect to reviewing your account statements and credit reports, and promptly report any suspicious activity or suspected identity theft to us and to the proper law enforcement authorities, including local law enforcement, your state's attorney general and/or the Federal Trade Commission ("FTC"). You may contact the FTC or your state's regulatory authority to obtain additional information about avoiding identity theft.

**Federal Trade Commission, Consumer Response Center**  
600 Pennsylvania Avenue, NW, Washington, DC 20580, 1-877-IDTHEFT (438-4338),  
[www.ftc.gov/idtheft](http://www.ftc.gov/idtheft)

We recommend that you regularly review the explanation of benefits statement that you receive from your insurer. If you see any service that you believe you did not receive, please contact your insurer at the number on the statement. If you do not receive regular explanation of benefits statements, contact your provider and request them to send such statements following the provision of services in your name or number.

You may want to order copies of your credit reports and check for any medical bills that you do not recognize. If you find anything suspicious, call the credit reporting agency at the phone number on the report. Keep a copy of this notice for your records in case of future problems with your medical records. You may also want to request a copy of your medical records from your provider, to serve as a baseline.

**Fraud Alerts:** There are also two types of fraud alerts that you can place on your credit report to put your creditors on notice that you may be a victim of fraud: an initial alert and an extended alert. You may ask that an initial fraud alert be placed on your credit report if you suspect you have been, or are about to be, a victim of identity theft. An initial fraud alert stays on your credit report for at least 90 days. You may have an extended alert placed on your credit report if you have already been a victim of identity theft with the appropriate documentary proof. An extended fraud alert stays on your credit report for seven years. You can place a fraud alert on your credit report by calling the toll-free fraud number of any of the three national credit reporting agencies listed below.

**Equifax:** 1-888-766-0008, [www.equifax.com](http://www.equifax.com)  
**Experian:** 1-888-397-3742, [www.experian.com](http://www.experian.com)  
**TransUnion:** 1-800-680-7289, [fraud.transunion.com](http://fraud.transunion.com)

**Credit Freezes:** You may have the right to put a credit freeze, also known as a security freeze, on your credit file, so that no new credit can be opened in your name without the use of a PIN number that is issued to you when you initiate a freeze. A credit freeze is designed to prevent potential credit grantors from accessing your credit report without your consent. If you place a credit freeze, potential creditors and other third parties will not be able to get access to your credit report unless you temporarily lift the freeze. Therefore, using a credit freeze may delay your ability to obtain credit. In addition, you may incur fees to



place, lift and/or remove a credit freeze. Credit freeze laws vary from state to state. The cost of placing, temporarily lifting, and removing a credit freeze also varies by state, generally \$5 to \$20 per action at each credit reporting company. *Unlike a fraud alert, you must separately place a credit freeze on your credit file at each credit reporting company.* Since the instructions for how to establish a credit freeze differ from state to state, please contact the three major credit reporting companies as specified below to find out more information:

Equifax:	P.O. Box 105788, Atlanta, GA 30348, <a href="http://www.equifax.com">www.equifax.com</a>
Experian:	P.O. Box 9554, Allen, TX 75013, <a href="http://www.experian.com">www.experian.com</a>
TransUnion LLC:	P.O. Box 2000, Chester, PA, 19022-2000, <a href="http://freeze.transunion.com">freeze.transunion.com</a>

You can obtain more information about fraud alerts and credit freezes by contacting the FTC or one of the national credit reporting agencies listed above.