



**WILSON ELSE**

WILSON ELSE MOSKOWITZ EDELMAN & DICKER LLP

STATE OF NH  
DEPT OF JUSTICE

2015 OCT 13 AM 11:36

Cons.

October 8, 2015

Melissa K. Ventrone  
312.821.6105 (direct)  
312.485.0540 (mobile)  
Melissa.Ventrone@wilsonelser.com

**Attorney General Joseph Foster**

Office of the Attorney General

33 Capitol Street

Concord, NH 03302

Re: Data Security Incident

Dear Attorney General Foster:

We represent Samela, Inc. d/b/a NorthShore Care Supply ("NorthShore") with respect to a recent security incident involving the potential exposure of certain personally identifiable information described in more detail below.

NorthShore Care Supply is supplier of incontinence products located in Buffalo Grove, Illinois. The vast majority of NorthShore's customer orders are placed via NorthShore's website, [www.NorthShoreCare.com](http://www.NorthShoreCare.com). NorthShore's e-commerce platform is hosted by a third party vendor that maintains and services the website and e-commerce platform.

**1. Nature of security incident.**

On August 24, 2015, NorthShore learned that its e-commerce website may have been compromised. NorthShore immediately hired independent computer security experts to assist with its investigation. While the investigation is still ongoing, it appears that one or more unauthorized individuals may have gained access to NorthShore's e-commerce platform hosted by the third party vendor and inserted malware that captured customers' names, addresses, credit and debit card numbers, security codes, and expiration dates at the point of check-out. Payment cards used to make purchases on NorthShore's website between June 7, 2015 and August 24, 2015 may have been affected.

**2. Number of New Hampshire residents affected.**

Forty three (43) New Hampshire residents were affected by the incident. A notification letter was sent to the affected individuals on October 8, 2015 via regular mail. A copy of the notification letter is included with this letter.

55 West Monroe Street, Suite 3800 • Chicago, IL 60603 • p 312.704.0550 • f 312.704.1522

Atlanta • Baltimore • Boston • Chicago • Dallas • Denver • Garden City • Hartford • Houston • Kentucky • Las Vegas • London • Los Angeles • Miami • Michigan  
Milwaukee • New Jersey • New York • Orlando • Philadelphia • San Diego • San Francisco • Stamford • Virginia • Washington, DC • West Palm Beach • White Plains

[wilsonelser.com](http://wilsonelser.com)

1928367v.1

**3. Steps you have taken or plan to take relating to the incident.**

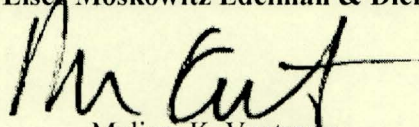
NorthShore has taken steps to prevent this type of event from happening again. This includes rebuilding the e-commerce website on a new server and enhancing the intrusion monitoring for the website. NorthShore is also offering potentially impacted individuals with identity restoration services through AllClear ID. Notice was also provided to the credit reporting agencies.

**4. Contact information.**

NorthShore remains dedicated to protecting the sensitive information in its systems. If you have any questions or need additional information, please do not hesitate to contact me at Melissa.Ventrone@wilsonelser.com or (312) 821-6105.

Very truly yours,

**Wilson Elser Moskowitz Edelman & Dicker LLP**

  
Melissa K. Ventrone

Enclosure





00255  
JOHN Q. SAMPLE  
1234 MAIN STREET  
ANYTOWN US 12345-6789

October 8, 2015

Dear John Sample:

We are writing to inform you of a data security incident that may have resulted in the disclosure of your credit or debit card information. We take the privacy and security of your information very seriously, and sincerely apologize for any concern or inconvenience this may cause you. This letter contains information about steps you can take to protect your information, and resources we are making available to help you.

On August 24, 2015, NorthShore Care Supply learned of a possible security incident involving its online ordering website. We immediately engaged independent IT forensic experts to assist with our investigation. While the investigation is still ongoing, it appears that your credit and debit card data may have been compromised if you made an online purchase between June 7, 2015 and August 24, 2015. The information potentially exposed includes your name, address, card number, verification code, and/or the card's expiration date.

Although we do not believe you are at risk for identity theft because the information at issue involves your credit or debit card information, we value you as a customer and 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 1-855-229-0069 and a dedicated investigator will do the work to recover financial losses, restore your credit and make sure your identity is returned to its proper condition.

**AllClear PLUS:** This service offers additional layers of protection including identity theft monitoring that delivers secure, actionable alerts to you by phone and \$1,000,000.00 Identity Theft Insurance Coverage. To use the PLUS service, you will need to provide your personal information to AllClear ID. You may sign up online at [enroll.allclearid.com](http://enroll.allclearid.com) or by phone by calling 1-855-229-0069 using the following redemption code Redemption Code.

Please note: Additional steps may be required by you in order to activate your phone alerts.

In addition to the steps we are taking, we suggest you monitor your credit or debit card and notify your bank if you notice any suspicious activity. Your trust is a top priority for NorthShore and we deeply regret any concern this may cause. The privacy and protection of your information is a matter we take



very seriously, and we have taken steps to prevent this type of event from occurring in the future. This includes rebuilding the e-commerce website on a new server and enhancing our website intrusion monitoring.

Again, we deeply regret any inconvenience or concern that this matter may cause you, and remain dedicated to protecting your information.

Sincerely,

A handwritten signature in black ink, appearing to read "Adam Greenberg". The signature is fluid and cursive, with the first name "Adam" being more prominent than the last name "Greenberg".

Adam Greenberg  
President  
NorthShore Care Supply

## **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 105139, Atlanta, Georgia 30374-0241, 1-800-685-1111, [www.equifax.com](http://www.equifax.com)

**Experian**, P.O. Box 2002, Allen, TX 75013, 1-888-397-3742, [www.experian.com](http://www.experian.com)

**TransUnion**, P.O. Box 6790, Fullerton, CA 92834-6790, 1-800-916-8800, [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)

**For residents of Maryland:** You may also obtain information about preventing and avoiding identity theft from the Maryland Office of the Attorney General:

**Maryland Office of the Attorney General**, Consumer Protection Division

200 St. Paul Place, Baltimore, MD 21202, 1-888-743-0023, [www.oag.state.md.us](http://www.oag.state.md.us)

**For residents of Massachusetts:** You also have the right to obtain a police report.

**For residents of North Carolina:** You may also obtain information about preventing and avoiding identity theft from the North Carolina Attorney General's Office:

**North Carolina Attorney General's Office**, Consumer Protection Division

9001 Mail Service Center, Raleigh, NC 27699-9001, 1-877-5-NO-SCAM, [www.ncdoj.gov](http://www.ncdoj.gov)

**The next 2 paragraphs are regarding incidents involving personal health information. Disregard if not applicable to your situation.**

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. If you are a California resident, we suggest that you visit the web site of the California Office of Privacy Protection at [www.privacy.ca.gov](http://www.privacy.ca.gov) to find more information about your medical privacy.

**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: 1-800-525-6285, [www.equifax.com](http://www.equifax.com)

Experian: 1-888-397-3742, [www.experian.com](http://www.experian.com)

TransUnion: 1-800-680-7289, [www.transunion.com](http://www.transunion.com)





**Credit Freezes (for Non-Massachusetts Residents):** 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, [www.equifax.com](http://www.equifax.com)  
Experian, P.O. Box 9554, Allen, TX 75013, [www.experian.com](http://www.experian.com)  
TransUnion, LLC, P.O. Box 2000, Chester, PA, 19022-2000, [www.transunion.com](http://www.transunion.com)

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.

**Credit Freezes (for Massachusetts Residents):** Massachusetts law gives you the right to place a security freeze on your consumer reports. A security freeze is designed to prevent credit, loans and services from being approved in your name without your consent. Using a security freeze, however, may delay your ability to obtain credit. You may request that a freeze be placed on your credit report by sending a request to a credit reporting agency by certified mail, overnight mail or regular stamped mail to the address below:

Equifax, P.O. Box 105788, Atlanta, GA 30348, [www.equifax.com](http://www.equifax.com)  
Experian, P.O. Box 9554, Allen, TX 75013, [www.experian.com](http://www.experian.com)  
TransUnion, LLC, P.O. Box 2000, Chester, PA, 19022-2000, [www.transunion.com](http://www.transunion.com)

*Unlike a fraud alert, you must separately place a credit freeze on your credit file at each credit reporting company.* The following information should be included when requesting a security freeze (documentation for you and your spouse must be submitted when freezing a spouse's credit report): full name, with middle initial and any suffixes; Social Security number; date of birth (month, day and year); current address and previous addresses for the past five (5) years; and applicable fee (if any) or incident report or complaint with a law enforcement agency or the Department of Motor Vehicles. The request should also include a copy of a government-issued identification card, such as a driver's license, state or military ID card, and a copy of a utility bill, bank or insurance statement. Each copy should be legible, display your name and current mailing address, and the date of issue (statement dates must be recent). The credit reporting company may charge a reasonable fee of up to \$5 to place a freeze or lift or remove a freeze, unless you are a victim of identity theft or the spouse of a victim of identity theft, and have submitted a valid police report relating to the identity theft to the credit reporting company.

## **AllClear Secure Terms of Use**

If you become a victim of fraud using your personal information without authorization, AllClear ID will help recover your financial losses and restore your identity. Benefits include:

- 12 months of coverage with no enrollment required;
- No cost to you – ever. AllClear Secure is paid for by the participating Company.

### **Services Provided**

If you suspect identity theft, simply call AllClear ID to file a claim. AllClear ID will provide appropriate and necessary remediation services ("Services") to help restore the compromised accounts and your identity to the state prior to the incident of fraud. Services are determined at the sole discretion of AllClear ID and are subject to the terms and conditions found on the AllClear ID website. AllClear Secure is not an insurance policy, and AllClear ID will not make payments or reimbursements to you for any financial loss, liabilities or expenses you incur.

### **Coverage Period**

Service is automatically available to you with no enrollment required for 12 months from the date of the breach incident notification you received from Company (the "Coverage Period"). Fraud events that occurred prior to your Coverage Period are not covered by AllClear Secure services.

### **Eligibility Requirements**

To be eligible for Services under AllClear Secure coverage, you must fully comply, without limitations, with your obligations under the terms herein, you must be a citizen or legal resident eighteen (18) years of age or older and have a valid U.S. Social Security number. Minors under eighteen (18) years of age may be eligible, but must be sponsored by a parent or guardian. The Services cover only you and your personal financial and medical accounts that are directly associated with your valid U.S. Social Security number, including but not limited to credit card, bank, or other financial accounts and/or medical accounts.

### **How to File a Claim**

If you become a victim of fraud covered by the AllClear Secure services (an "Event"), you must:

- notify AllClear ID by calling 1.855.434.8077 to report the fraud prior to expiration of your Coverage Period;
- provide proof of eligibility for AllClear Secure by providing the redemption code on the notification letter you received from the sponsor Company;
- fully cooperate and be truthful with AllClear ID about the Event and agree to execute any documents AllClear ID may reasonably require; and
- fully cooperate with AllClear ID in any remediation process, including, but not limited to, providing AllClear ID with copies of all available investigation files or reports from any institution, including, but not limited to, credit institutions or law enforcement agencies, relating to the alleged theft.

### **Coverage Under AllClear Secure Does Not Apply to the Following:**

Any expense, damage or loss:

- due to
  - any transactions on your financial accounts made by authorized users, even if acting without your knowledge, or
  - any act of theft, deceit, collusion, dishonesty or criminal act by you or any person acting in concert with you, or by any of your authorized representatives, whether acting alone or in collusion with you or others (collectively, your "Misrepresentation");
- incurred by you from an Event that did not occur during your coverage period; or
- in connection with an Event that you fail to report to AllClear ID prior to the expiration of your AllClear Secure coverage period.

### **Other Exclusions:**

- AllClear ID will not pay or be obligated for any costs or expenses other than as described herein, including without limitation, fees of any service providers not retained by AllClear ID; AllClear ID reserves the right to investigate any asserted claim to determine its validity.
- AllClear ID is not an insurance company, and AllClear Secure is not an insurance policy; AllClear ID will not make payments or reimbursements to you for any loss or liability you may incur.
- AllClear ID is not a credit repair organization, is not a credit counseling service, and does not promise to help you improve your credit history or rating beyond resolving incidents of fraud.
- AllClear ID reserves the right to reasonably investigate any asserted claim to determine its validity. All recipients of Secure coverage are expected to protect their personal information in a reasonable way at all times. Accordingly, recipients will not deliberately or recklessly disclose or publish their Social Security number or any other personal information to those who would reasonably be expected to improperly use or disclose that Personal Information.

### **Opt-out Policy**

If for any reason you wish to have your information removed from the eligibility database for AllClear Secure, please contact AllClear ID:

<b><u>E-mail</u></b>	<b><u>Mail</u></b>	<b><u>Phone</u></b>
support@allclearid.com	AllClear ID, Inc. 823 Congress Avenue Suite 300 Austin, Texas 78701	1.855.434.8077

