mwe.com

Edward Zacharias
Attorney at Law
ezacharias@mwe.com
+1 617 535 4018

June 4, 2019

VIA EMAIL
Attorney General Gordon MacDonald
Attn: Consumer Protection and Antitrust Bureau
33 Capitol Street
Concord, NH 03301
DOJ-CPB@doj.nh.gov

Re: Steward – Security Incident Notification

Dear Attorney General MacDonald:

We represent Steward Health Care System LLC ("Steward") with respect to an incident involving the potential exposure of certain personal information described in detail below. Steward is a large healthcare network that serves patients throughout the United States. Unfortunately, it appears that the personal information of certain Steward vendors may have been exposed in a cyber attack. At this time, there is no indication that any of the personal information has been misused. We have retained a leading cybersecurity forensic vendor to assist with the investigation, which is ongoing.

1. Nature of the Security Incident

On April 12, 2019, Steward learned that a cyber-attacker may have gained access to the email account of a Steward employee. Earlier on that day, the attacker appears to have sent an email from the employee's account to another Steward employee requesting the payment of an invoice via money wire transfer. Steward identified that the employee had not sent this email and immediately initiated an investigation into the situation. The investigation is ongoing. Steward used a software tool to scan the employee's email mailbox in an effort to determine whether the mailbox may have contained any personal information or protected health information. On April 26, 2019, the scan discovered an email located in the employee's mailbox containing an attachment that included the names, addresses, and employee identification numbers ("EINs") of certain Steward vendors. Some of these vendors were sole proprietors who we suspect use their Social Security number as their EIN.

2. Steps Taken in Response to the Security Incident

Immediately upon learning of the situation, Steward initiated an investigation and took steps to eradicate the attacker from its network. Steward promptly reset the employee's email account password and temporarily disabled the account as it was analyzed. A leading cybersecurity forensic vendor was engaged to conduct a robust forensic investigation. Steward's investigation into this matter continues. Steward

will provide 12 months of complementary credit monitoring and other identity theft protection services to the affected individuals.

3. Number of New Hampshire Residents Impacted

Steward has identified 81 New Hampshire residents who we suspect were potentially impacted by this incident. A notification letter will be sent to each of these individuals on June 4, 2019 via regular mail. A copy of the form notification letter is enclosed.

4. Contact Information

Please contact me at ezacharias@mwe.com or 617-535-4018 if you have any questions.

Sincerely,

Edward G. Zacharias

June 4, 2019

«Title» «First_Name» «Last_Name»
«Street_Address»
«City» «State» «Zip»

NOTICE OF DATA BREACH

Dear «Title» «Last_Name»:

We are sending you this notice because of a recent data security incident that occurred at Steward Health Care System LLC (Steward) that may have involved your personal information. At this time, we are not aware of any misuse of your information.

WHAT HAPPENED?
On April 12, 2019, we became aware that an unauthorized person gained access to an email account of a Steward employee. Upon learning of the situation, we took immediate action to contain the incident and to prevent any further unauthorized access. After an extensive review, on April 26, 2019 we discovered that an email attachment located in the employee's email account contained certain information about you as a vendor to Steward. We are conducting an extensive forensic investigation into the matter, and thus far, we found no evidence that the unauthorized person accessed the file with your information.

WHAT INFORMATION WAS INVOLVED?
The information included in the email attachment contained your name, address, and your employer identification number (EIN)—also known as you tax identification number (TIN). Depending on how you established your EIN/TIN with the Internal Revenue Service, your EIN/TIN may be your Social Security number.

WHAT WE ARE DOING
Steward takes the protection of our vendor's personal information very seriously and we are committed to protecting it. Upon learning of the situation, we immediately began an investigation, quickly terminated the unauthorized person's access, and enlisted the assistance of a leading cybersecurity forensics firm to investigation this matter. The investigation is ongoing and Steward will assess the findings of the investigation as part of our persistent efforts to identify and prevent cybersecurity threats.

As noted above, there is no indication that your personal information has been misused at this time. Nevertheless, as an added precaution, Steward would like to offer you 12 months of credit monitoring from Experian at no cost to you. If you would like to put such monitoring in place, you can activate the credit monitoring product by taking the following steps no later than August 17, 2019.

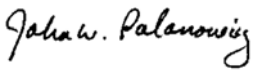
1. VISIT the Web Site https://www.experianidworks.com/3bcredit or call 877-288-8057.
2. PROVIDE your Activation Code: «CODE» and Engagement Number: [redacted]

WHAT YOU CAN DO
In addition to enrolling in the identity monitoring services we have arranged on your behalf, we encourage you to review the "General Information About Identity Theft Protection" sheet enclosed with this letter. You should always remain vigilant for threats of fraud and identity theft by regularly reviewing your account statements and credit reports.

FOR MORE INFORMATION

We apologize for any inconvenience that this incident may cause you. If you have any questions or concerns, please contact us 888-675-0090.

Sincerely,



John Polanowicz
Chief Operating Officer
Steward Health Care System LLC

GENERAL INFORMATION ABOUT IDENTITY THEFT PROTECTION

You should remain vigilant for incidents of fraud and identity theft by reviewing credit card account statements and monitoring your credit report for unauthorized activity.

Credit Reports. Under federal law, you are entitled to one free copy of your credit report every 12 months from each of the three nationwide credit reporting agencies. You may obtain a free copy of your credit report by going to www.AnnualCreditReport.com or by calling (877) 322-8228. You also may complete the Annual Credit Report Request Form available from the FTC at www.consumer.ftc.gov/articles/pdf-0093-annual-report-request-form.pdf, and mail it to Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA 30348-5281.

You may contact the nationwide credit reporting agencies at:

Equifax	Experian	TransUnion
P.O. Box 105788 Atlanta, GA 30348 www.equifax.com (800) 525-6285	P.O. Box 9554 Allen, TX 75013 www.experian.com (888) 397-3742	P.O. Box 2000 Chester, PA 19016 www.transunion.com (800) 680-7289

Fraud Alert. You may place a fraud alert in your file by calling one of the three nationwide credit reporting agencies above. A fraud alert tells creditors to follow certain procedures, including contacting you before they open any new accounts or change your existing accounts. For that reason, placing a fraud alert can protect you, but also may delay you when you seek to obtain credit.

Place a Security Freeze on your Credit Report. You also have the right to place a security freeze on your credit report by contacting any of the credit bureaus listed at above. A security freeze is intended to prevent credit, loans and services from being approved in your name without your consent. To place a security freeze on your credit report, you may be able to use an online process, an automated telephone line or a written request. The following information must be included when requesting a security freeze (note that if you are requesting a credit report for your spouse, this information must be provided for him/her as well): (1) full name, with middle initial and any suffixes; (2) Social Security number; (3) date of birth; (4) current address and any previous addresses for the past five years; and (5) any applicable incident report or complaint with a law enforcement agency or the Registry of Motor Vehicles. The request must also include a copy of a government-issued identification card and a copy of a recent utility bill or bank or insurance statement. It is essential that each copy be legible, display your name and current mailing address, and the date of issue. The consumer reporting agency may charge a fee of up to $5.00 to place a freeze or lift or remove a freeze and free if you are a victim of identity theft or the spouse of a victim of identity theft, and you have submitted a valid police report relating to the identity theft incident to the consumer reporting agency.

You may contact the Federal Trade Commission (FTC) and State Attorneys General Offices. If you believe you are the victim of identity theft or have reason to believe your personal information has been misused, you should contact the FTC and/or your state's attorney general office about for information on how to prevent or avoid identity theft. You can contact the FTC at: **Federal Trade Commission**, Consumer Response Center, 600 Pennsylvania Avenue, NW, Washington, DC 20508, www.ftc.gov, 1-877-IDTHEFT (438-4338).

If you are an Iowa resident, state law advises you to report any suspected identity theft to law enforcement or to the Iowa Attorney General, Consumer Protection Division, 1305 E. Walnut St., Des Moines, IA 50319, 1-888-777-4590.

If you are a Maryland resident, you can contact the Maryland Office of the Attorney General, Consumer Protection Division at: 200 St. Paul Place, Baltimore, MD 21202, www.oag.state.md.us, 1-888-743-0023

If you are a New Mexico resident, you have certain rights pursuant to the federal Fair Credit Reporting Act (FCRA). For more information about the FCRA, please visit www.consumer.ftc.gov/articles/pdf-0096-fair-credit-reporting-act.pdf or www.ftc.gov.

If you are a North Carolina resident, you can contact the North Carolina Office of the Attorney General, Consumer Protection Division at: 9001 Mail Service Center, Raleigh, NC 27699-9001, www.ncdoj.com, 1-877-566-7226

If you are an Oregon resident, state law advises you to report any suspected identity theft to law enforcement or to the FTC.

If you are a Rhode Island resident, you can contact the Office of the Attorney General at: Rhode Island Office of the Attorney General, 150 South Main Street, Providence, RI 02903, http://www.riag.ri.gov/, (401) 274-4400.