MULLEN COUGHLIN LLC
ATTORNEYS AT LAW

Christopher J. DiIenno
Office: (267) 930-4775
Fax: (267) 930-4771
Email: cdiienno@mullen.law

1275 Drummers Lane, Suite 302
Wayne, PA 19087

August 8, 2019

VIA U.S. MAIL

Attorney General Gordon J. MacDonald
Office of the New Hampshire Attorney General
Consumer Protection Bureau
33 Capitol Street
Concord, NH 03301

Re: Notice of Data Event

Dear Attorney General McDonald:

We represent St. Croix Hospice located at 7755 3rd St N, Suite #200, Oakdale, Minnesota 55128, and write to notify your office of an incident that may affect the security of some personal information relating to three (3) New Hampshire residents. The investigation into this matter is ongoing, and this notice will be supplemented with any new significant facts learned subsequent to its submission. By providing this notice, St. Croix Hospice does not waive any rights or defenses regarding the applicability of New Hampshire law, the applicability of the New Hampshire data event notification statute, or personal jurisdiction.

Nature of the Data Event

On May 10, 2019, St. Croix Hospice noticed suspicious activity in a certain email account. St. Croix Hospice immediately began an investigation into the activity. This investigation included working with third-party forensic investigators to confirm the nature and scope of this incident. On May 30, 2019, the investigation determined that there was unauthorized access to certain email accounts between April 23, 2019 and May 11, 2019. The investigation was unable to determine what information, if any, was accessed within those email accounts.

In an abundance of caution, St. Croix Hospice began reviewing the affected email accounts to determine if there was any personal information present in the accounts at the time of the incident. This review required an extensive systematic and manual review of the emails, files and documents. On June 21, 2019, St. Croix Hospice determined that personal information was present in the affected email accounts at the time of the incident. Since that time, St. Croix Hospice has

been diligently reviewing its records and the involved emails for purposes of notifying affected individuals. St. Croix Hospice's investigation has not revealed evidence of actual or attempted misuse of personal information as a result of this incident.

The information that could have been subject to unauthorized access includes name, address, date of birth, Medicare/Medicaid number, and medical information.

Notice to New Hampshire Residents

On or about June 21, 2019, St. Croix Hospice began providing written notice of this incident to affected individuals, which includes three (3) New Hampshire residents. Written notice is being provided in substantially the same form as the letter attached here as ***Exhibit A***.

Other Steps Taken and To Be Taken

Upon discovering the event, St. Croix Hospice moved quickly to investigate and respond to the incident, assess the security of St. Croix Hospice systems, and notify potentially affected individuals. St. Croix Hospice is also working to implement additional safeguards and training to its employees. St. Croix Hospice is providing access to credit monitoring services for 12 months through TransUnion, to individuals whose personal information was potentially affected by this incident, at no cost to these individuals.

Additionally, St. Croix Hospice is providing impacted individuals with guidance on how to better protect against identity theft and fraud, including advising individuals to report any suspected incidents of identity theft or fraud to their credit card company and/or bank. St. Croix Hospice is providing individuals with information on how to place a fraud alert and security freeze on one's credit file, the contact details for the national consumer reporting agencies, information on how to obtain a free credit report, a reminder to remain vigilant for incidents of fraud and identity theft by reviewing account statements and monitoring free credit reports, and encouragement to contact the Federal Trade Commission, their state Attorney General, and law enforcement to report attempted or actual identity theft and fraud. St. Croix Hospice also notified the Department of Health and Human Services and appropriate state regulators.

Contact Information

Should you have any questions regarding this notification or other aspects of the data security event, please contact us at (267) 930-4775.

Very truly yours,

Christopher J. DiIenno of
MULLEN COUGHLIN LLC

EXHIBIT A

ST. CROIX
HOSPICE

Return Mail Processing Center
PO Box 6336
Portland, OR 97228-6336

<<Mail ID>>
<<Name 1>>
<<Name 2>>
<<Address 1>>
<<Address 2>>
<<Address 3>>
<<Address 4>>
<<Address 5>>
<<City>><<State>><<Zip>>
<<Country>>

<<Date>>

Dear <<Name1>>:

St. Croix Hospice writes to make you aware of a data privacy incident that may have impacted the security of your protected health information. While St. Croix Hospice's investigation has not revealed evidence of actual or attempted misuse of any personal information as a result of this incident, we wanted you to be aware of the incident, our response, and steps you may take to protect against possible misuse of your personal information, should you feel it appropriate to do so.

What Happened? On May 10, 2019, St. Croix Hospice noticed suspicious activity in a certain email account. St. Croix Hospice immediately began an investigation into the activity. This investigation included working with third-party forensic investigators to confirm the nature and scope of this incident. On May 30, 2019, the investigation determined that there was unauthorized access to certain email accounts between April 23, 2019 and May 11, 2019. The investigation was unable to determine what information, if any, was accessed within those email accounts.

In an abundance of caution, St. Croix Hospice began to review the affected email accounts to determine if there was any protected health information present in the accounts at the time of the incident. This review required an extensive systematic and manual review of the emails, files and documents. On June 21, 2019, St. Croix Hospice determined that personal information was present in the affected email accounts at the time of the incident. Since that time, St. Croix Hospice has been diligently reviewing its records for purposes of notifying affected individuals. St. Croix Hospice's investigation has not revealed evidence of actual or attempted misuse of protected health information as a result of this incident.

What Information Was Involved? Our investigation confirmed the affected email accounts contained sensitive information including your name, <<Variable Data>>. Please note that while our investigation did not reveal evidence that this information was actually accessed or viewed during the incident, we are providing you this notice to ensure you are aware of this incident.

What We Are Doing. The confidentiality, privacy, and security of information is one of our highest priorities. Upon learning of this incident, we immediately took steps to assess the security of our systems and conduct a thorough investigation. In response to this incident, we are reviewing our security policies and procedures and taking various steps to improve our existing technical, administrative, and physical safeguards. In addition, St. Croix Hospice notified appropriate state regulators and the Department of Health and Human Services of this incident.

What You Can Do. You may review the enclosed "Steps You Can Take to Protect Against Identity Theft and Fraud," which contains information on what you can do to protect against possible misuse of your information.

For More Information. We understand you may have questions that are not answered in this letter. If you have questions, please contact our dedicated call center at 877-330-3463 Monday through Friday from 8:00 a.m. to 8:00 p.m. Central Time.

Sincerely,

Kimberly Olson
Chief Compliance Office
St. Croix Hospice

Steps You Can Take to Protect Against Identity Theft and Fraud

As a safeguard, we have arranged for you to enroll, at no cost to you, in an online credit monitoring service (*my*TrueIdentity) for one year provided by TransUnion Interactive, a subsidiary of TransUnion,® one of the three nationwide credit reporting companies.

How to Enroll: You can sign up online or via U.S. mail delivery

- To enroll in this service, go to the *my*TrueIdentity website at **www.MyTrueIdentity.com** and, in the space referenced as "Enter Activation Code," enter the 12-letter Activation Code **<<Insert Unique 12-letter Activation Code>>** and follow the three steps to receive your credit monitoring service online within minutes.
- If you do not have access to the Internet and wish to enroll in a similar offline, paper-based credit monitoring service, via U.S. mail delivery, please call the TransUnion Fraud Response Services toll-free hotline at **1-855-288-5422**. When prompted, enter the six-digit telephone passcode **<<Insert static 6-digit Telephone Pass Code>>** and follow the steps to enroll in the offline credit monitoring service, add an initial fraud alert to your credit file, or to speak to a TransUnion representative if you believe you may be a victim of identity theft.

You can sign up for the online or offline credit monitoring service anytime between now and **<<Enrollment Deadline>>**. Due to privacy laws, we cannot register you directly. Please note that credit monitoring services might not be available for individuals who do not have a credit file with TransUnion or an address in the United States (or its territories) and a valid Social Security number. Enrolling in this service will not affect your credit score.

ADDITIONAL DETAILS REGARDING YOUR 12-MONTH COMPLIMENTARY CREDIT MONITORING SERVICE:

- Once you are enrolled, you will be able to obtain one year of unlimited access to your TransUnion credit report and credit score.
- The daily credit monitoring service will notify you if there are any critical changes to your credit file at TransUnion, including fraud alerts, new inquiries, new accounts, new public records, late payments, changes of address, and more.
- The service also includes access to an identity restoration program that provides assistance in the event that your identity is compromised and up to $1,000,000 in identity theft insurance with no deductible. (Policy limitations and exclusions may apply.)

We encourage you to remain vigilant against incidents of identity theft and fraud, to review your account statements, and to monitor your credit reports for suspicious activity. Under U.S. law you are entitled to one free credit report annually from each of the three major credit reporting bureaus. To order your free credit report, visit www.annualcreditreport.com or call, toll-free, 1-877-322-8228. You may also contact the three major credit bureaus directly to request a free copy of your credit report.

You have the right to place a "security freeze" on your credit report, which will prohibit a consumer reporting agency from releasing information in your credit report without your express authorization. The security freeze is designed to prevent credit, loans, and services from being approved in your name without your consent. However, you should be aware that using a security freeze to take control over who gets access to the personal and financial information in your credit report may delay, interfere with, or prohibit the timely approval of any subsequent request or application you make regarding a new loan, credit, mortgage, or any other account involving the extension of credit. Pursuant to federal law, you cannot be charged to place or lift a security freeze on your credit report. Should you wish to place a security freeze, please contact the major consumer reporting agencies listed below:

Experian **PO Box 9554** **Allen, TX 75013** **1-888-397-3742** **www.experian.com/freeze/center.html**	**TransUnion** **P.O. Box 2000** **Chester, PA 19016** **1-888-909-8872** **www.transunion.com/credit-freeze**	**Equifax** **PO Box 105788** **Atlanta, GA 30348-5788** **1-800-685-1111** **www.equifax.com/personal/credit-report-services**

In order to request a security freeze, you will need to provide the following information:

1. Your full name (including middle initial as well as Jr., Sr., II, III, etc.);
2. Social Security number;
3. Date of birth;
4. If you have moved in the past five (5) years, provide the addresses where you have lived over the prior five years;
5. Proof of current address, such as a current utility bill or telephone bill;
6. A legible photocopy of a government-issued identification card (state driver's license or ID card, military identification, etc.);
7. If you are a victim of identity theft, include a copy of either the police report, investigative report, or complaint to a law enforcement agency concerning identity theft.

As an alternative to a security freeze, you have the right to place an initial or extended "fraud alert" on your file at no cost. An initial fraud alert is a 1-year alert that is placed on a consumer's credit file. Upon seeing a fraud alert display on a consumer's credit file, a business is required to take steps to verify the consumer's identity before extending new credit. If you are a victim of identity theft, you are entitled to an extended fraud alert, which is a fraud alert lasting seven years. Should you wish to place a fraud alert, please contact any one of the agencies listed below:

Experian	**TransUnion**	**Equifax**
P.O. Box 2002	P.O. Box 2000	P.O. Box 105069
Allen, TX 75013	Chester, PA 19016	Atlanta, GA 30348
1-888-397-3742	1-800-680-7289	1-888-766-0008
www.experian.com/fraud/center.html	www.transunion.com/fraud-victim-resource/place-fraud-alert	www.equifax.com/personal/credit-report-services

Additional Information

You can further educate yourself regarding identity theft, fraud alerts, security freezes, and the steps you can take to protect yourself, by contacting the consumer reporting agencies, the Federal Trade Commission, or your state Attorney General.

The Federal Trade Commission can be reached at: 600 Pennsylvania Avenue NW, Washington, DC 20580, www.identitytheft.gov, 1-877-ID-THEFT (1-877-438-4338); TTY: 1-866-653-4261. The Federal Trade Commission also encourages those who discover that their information has been misused to file a complaint with them. You can obtain further information on how to file such a complaint by way of the contact information listed above. You have the right to file a police report if you ever experience identity theft or fraud. Please note that in order to file a report with law enforcement for identity theft, you will likely need to provide some proof that you have been a victim. Instances of known or suspected identity theft should also be reported to law enforcement and your state Attorney General. This notice has not been delayed by law enforcement.

For Maryland residents, the Attorney General can be contacted at 200 St. Paul Place, 16th Floor, Baltimore, MD 21202, 1-888-743-0023, www.oag.state.md.us. St. Croix Hospice is located at 7755 3rd Street N, Suite #200, Oakdale, Minnesota, 55128-5442.

For New Mexico residents, you have rights pursuant to the Fair Credit Reporting Act, such as the right to be told if information in your credit file has been used against you, the right to know what is in your credit file, the right to ask for your credit score, and the right to dispute incomplete or inaccurate information. Further, pursuant to the Fair Credit Reporting Act, the consumer reporting agencies must correct or delete inaccurate, incomplete, or unverifiable information; consumer reporting agencies may not report outdated negative information; access to your file is limited; you must give your consent for credit reports to be provided to employers; you may limit "prescreened" offers of credit and insurance you get based on information in your credit report; and you may seek damages from violator. You may have additional rights under the Fair Credit Reporting Act not summarized here. Identity theft victims and active duty military personnel have specific additional rights pursuant to the Fair Credit Reporting Act. We encourage you to review your rights pursuant to the Fair Credit Reporting Act by visiting www.consumerfinance.gov/f/201504_cfpb_summary_your-rights-under-fcra.pdf, or by writing Consumer Response Center, Room 130-A, Federal Trade Commission, 600 Pennsylvania Ave. N.W., Washington, D.C. 20580.

For North Carolina residents, the Attorney General can be contacted at 9001 Mail Service Center, Raleigh, NC 27699-9001, 1-877-566-7226 or 1-919-716-6400, www.ncdoj.gov.