



Melissa K. Ventrone
T (312) 360-2506
F (312) 517-7572
Email: mventrone@ClarkHill.com

Clark Hill
130 E. Randolph Street, Suite 3900
Chicago, Illinois 60601
T (312) 985-5900
F (312) 985-5900

January 14, 2022

Via Regular Mail

Office of the Attorney General
Identity Theft Unit
200 St. Paul Place
Baltimore, MD 21202



Dear Attorney General Brian E. Frosh,

We represent Catholic Hospice with respect to a data security incident described in more detail below. Catholic Hospice is committed to answering any questions you may have about the data security incident, its response, and steps taken to prevent a similar incident in the future.

1. Nature of security incident

During a separate and unrelated investigation, Catholic Hospice determined that email accounts for three Catholic Hospice employees may have been compromised. Catholic Hospice engaged an independent computer forensic firm to review the information in the accounts to identify and extract any protected health information, and on December 1, 2021, learned that personal information was present in the accounts. Information that may have been impacted includes names, addresses, and some combination of the following: demographic information, Social Security numbers, medical information and treatment history, diagnosis, and other health related information.

2. Number of residents affected

Eighteen (18) Maryland residents may have been affected and were notified of the incident. A notification letter was sent to the potentially affected individuals on January 14, 2022 via regular mail (a copy of the form notification letter is enclosed).

3. Steps taken in response to the incident

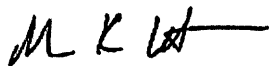
In response to this incident, Catholic Hospice engaged independent computer forensic experts to assist with determining the scope and impact of the incident and changed passwords on the impacted accounts. In addition, they have arranged for affected individuals to receive credit monitoring and identity protection services provided by IDX. Notice has also been provided to the Department of Health and Human Services, Office of Civil Rights.

January 14, 2022
Page 2

4. Contact information

Catholic Hospice takes the security of the information in its control seriously and is committed to ensuring the information in its control is appropriately protected. If you have any questions or need additional information, please do not hesitate to contact me at mventrone@clarkhill.com or (312) 360-2506.

Sincerely,
CLARK HILL

A handwritten signature in black ink, appearing to read "M K Ventrone", with a horizontal line extending to the right.

Melissa K. Ventrone
Member

CC: Paul Schmeltzer



P.O. Box 1907
Suwanee, GA 30024

To Enroll, Please Call:
(833) 676-2225
Or Visit:
<https://response.idx.us/hospice>
Enrollment Code: [XXXXXXXXX]

<FirstName> <LastName>
<Address1>
<Address2>
<City><State><Zip>

January 14, 2022

Notice of Data Security Incident

Dear NAME:

We are writing to inform you of a recent data security incident experienced by Catholic Hospice that may have impacted your personal information described in more detail below. We take the privacy and security of your information 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.

What Happened:

During a separate investigation, Catholic Hospice determined that email accounts for three Catholic Hospice employees may have been compromised. Catholic Hospice engaged an independent computer forensic firm to review the information in the account to identify and extract any protected health information, and on December 1, 2021, learned that your information was present in the accounts.

What Information Was Involved:

Information that may have been impacted includes your name, Social Security number, and some combination of your date of birth, demographic information, diagnosis and treatment information, Medical Record Number and other health care related information.

What We Are Doing:

We want to assure you that we are taking steps to minimize the risk of this kind of event from happening in the future. In response to the incident, we engaged independent computer forensic experts to assist with determining the scope and impact of the incident, and changed passwords on the accounts. In addition, we have arranged for you to receive credit monitoring and identity protection services provided by IDX. IDX services include: 12 months of Credit and CyberScan monitoring, a \$1,000,000 insurance reimbursement policy, and fully managed ID theft recovery services. With this protection, IDX will help you resolve issues if your identity is compromised.

What You Can Do:

We encourage you to enroll in free IDX identity protection services by going to <https://response.idx.us/hospice> or calling (833) 676-2225 and using the Enrollment Code provided above. IDX representatives are available Monday through Friday from 6 am - 6 pm Pacific Time. Please note the deadline to enroll is April 14, 2022.

Please review the enclosure included with this letter which describes additional steps you can take to help protect your identity, including recommendations by the Federal Trade Commission regarding identity theft protection and details on how to place a fraud alert or a security freeze on your credit file.

For more information.

If you have any questions or concerns, please call (833) 676-2225 Monday through Friday from 6 am - 6 pm Pacific Time. Also, you will need to reference the enrollment code at the top of this letter when enrolling, so please do not discard this letter.

Your trust is a top priority for us, and we deeply regret any inconvenience or concern that this matter may cause you.

Sincerely,

Catholic Hospice

RECOMMENDED STEPS TO HELP PROTECT YOUR INFORMATION

1. Website and Enrollment. Go to <https://response.idx.us/hospice> and follow the instructions for enrollment using your Enrollment Code provided at the top of the letter.

2. Activate the credit monitoring provided as part of your IDX identity protection membership. The monitoring included in the membership must be activated to be effective. Note: You must have established credit and access to a computer and the internet to use this service. If you need assistance, IDX will be able to assist you.

3. Telephone. Contact IDX at (833) 676-2225 to gain additional information about this event and speak with knowledgeable representatives about the appropriate steps to take to protect your credit identity.

4. Review your credit reports. We recommend that you remain vigilant by reviewing account statements and monitoring credit reports. Under federal law, you also are entitled every 12 months to one free copy of your credit report from each of the three major credit reporting companies. To obtain a free annual credit report, go to www.annualcreditreport.com or call 1-877-322-8228. You may wish to stagger your requests so that you receive a free report by one of the three credit bureaus every four months.

If you discover any suspicious items and have enrolled in IDX identity protection, notify them immediately by calling or by logging into the IDX website and filing a request for help.

If you file a request for help or report suspicious activity, you will be contacted by a member of our ID Care team who will help you determine the cause of the suspicious items. In the unlikely event that you fall victim to identity theft as a consequence of this incident, you will be assigned an ID Care Specialist who will work on your behalf to identify, stop and reverse the damage quickly.

You should also know that you have the right to file a police report if you ever experience identity fraud. Please note that in order to file a crime report or incident report with law enforcement for identity theft, you will likely need to provide some kind of proof that you have been a victim. A police report is often required to dispute fraudulent items. You can report suspected incidents of identity theft to local law enforcement or to the Attorney General.

5. Place Fraud Alerts with the three credit bureaus. If you choose to place a fraud alert, we recommend you do this after activating your credit monitoring. You can place a fraud alert at one of the three major credit bureaus by phone and also via Experian's or Equifax's website. 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. The contact information for all three bureaus is as follows:

Credit Bureaus

Equifax Fraud Reporting
P.O. Box 105069
Atlanta, GA 30348-5069

Equifax Credit Freeze
P.O. Box 105788
Atlanta, GA 30348-5788
1-888-836-6351
www.equifax.com/personal/credit-report-services

Experian Fraud Reporting and
Credit Freeze
P.O. Box 9554
Allen, TX 75013
1-888-397-3742
www.experian.com

TransUnion Fraud Reporting
P.O. Box 2000
Chester, PA 19022-2000

TransUnion Credit Freeze
P.O. Box 160
Woodlyn, PA 19094
1-800-680-7289
www.transunion.com

It is necessary to contact only ONE of these bureaus and use only ONE of these methods. As soon as one of the three bureaus confirms your fraud alert, the others are notified to place alerts on their records as well. You will receive confirmation letters in the mail and will then be able to order all three credit reports, free of charge, for your review. An initial fraud alert will last for one year.

Please Note: No one is allowed to place a fraud alert on your credit report except you.

6. Security Freeze. By placing a security freeze, someone who fraudulently acquires your personal identifying information will not be able to use that information to open new accounts or borrow money in your name. You will need to contact the three national credit reporting bureaus listed above to place the freeze. Keep in mind that when you place the freeze, you will not be able to borrow money, obtain instant credit, or get a new credit card until you temporarily lift or permanently remove the freeze. There is no cost to freeze or unfreeze your credit files.

7. You can obtain additional information about the steps you can take to avoid identity theft from the following agencies. The Federal Trade Commission also encourages those who discover that their information has been misused to file a complaint with them.

California Residents: Visit the California Office of Privacy Protection (www.oag.ca.gov/privacy) for additional information on protection against identity theft.

District of Columbia: Office of the Attorney General, 400 6th Street, NW, Washington, DC 20001; 202-727-3400; oag@dc.gov.

Maryland Residents: Office of the Attorney General of Maryland, Consumer Protection Division 200 St. Paul Place Baltimore, MD 21202, www.oag.state.md.us/Consumer, Telephone: 1-888-743-0023.

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 a 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. You can review your rights pursuant to the Fair Credit Reporting Act by visiting www.consumerfinance.gov/f/201904_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.

New York Residents: the Attorney General may be contacted at: Office of the Attorney General, The Capitol, Albany, NY 12224-0341; 1-800-771-7755; <https://ag.ny.gov/>.

North Carolina Residents: Office of the Attorney General of North Carolina, 9001 Mail Service Center Raleigh, NC 27699-9001, www.ncdoj.gov, Telephone: 1-919-716-6400.

Oregon Residents: Oregon Department of Justice, 1162 Court Street NE, Salem, OR 97301-4096, www.doj.state.or.us/, Telephone: 877-877-9392.

Rhode Island Residents: Office of the Attorney General, 150 South Main Street, Providence, Rhode Island 02903, www.riag.ri.gov, Telephone: 401-274-4400. You have the right to obtain any police report filed in regard to this incident. There are [XX] Rhode Island residents impacted by this incident.

All US Residents: Identity Theft Clearinghouse, Federal Trade Commission, 600 Pennsylvania Avenue, NW Washington, DC 20580, www.consumer.gov/idtheft, 1-877-IDTHEFT (438-4338), TTY: 1-866-653-4261.