RECEIVED
NOV 08 2022
CONSUMER PROTECTION

MULLEN COUGHLIN LLC
ATTORNEYS AT LAW

Colin D. Scanlon
Office: (267) 930-4259
Fax: (267) 930-4771
Email: cscanlon@mullen.law

426 W. Lancaster Avenue, Suite 200
Devon, PA 19333

November 4, 2022

VIA U.S. MAIL

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

Re: Notice of Data Event

Dear Sir or Madam:

We represent General Health System, Inc. ("GHS") located at 8595 Picardy Avenue, Suite 100, Baton Rouge, LA 70809, and are writing to notify your office of an incident that may affect the security of certain personal information relating to three (3) New Hampshire residents. This notice may be supplemented with new significant facts learned subsequent to its submission. By providing this notice, GHS 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 June 28, 2022, GHS became aware of suspicious activity related to certain GHS's computer systems. GHS immediately launched an investigation, with the assistance of third-party forensic specialists, to determine the nature and scope of the activity. Through the investigation, it was determined that there was unauthorized access to GHS's network between June 24, 2022 to June 29, 2022. The unauthorized actor had the ability to access certain directories while on the network. Therefore, GHS undertook a comprehensive review of the contents of the directories determined to be at risk to assess what sensitive information was contained within them and to whom the information related. On October 13, 2022, GHS completed its review and determined certain individuals could be affected. The information that could have been subject to unauthorized access includes name, Social Security number, date of birth, and medical diagnosis/treatment information.

Notice to New Hampshire Residents

On or about November 4, 2022, GHS 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 hereto as ***Exhibit A***. GHS also provided notice of the incident on its website and published a media notice throughout the state of Louisiana on August 24, 2022.

Other Steps Taken and To Be Taken

Upon discovering the event, GHS moved quickly to investigate, respond to the incident, assess the security of its systems, and identify potentially affected individuals. GHS also implemented additional data security safeguards. GHS is providing individuals whose personal information was potentially affected by this incident with access to credit monitoring and identity restoration services through Equifax for one (1) year at no cost to the individuals.

Additionally, GHS is providing impacted individuals with guidance on how to better protect against identity theft and fraud. GHS is also 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.

GHS notified applicable state regulators and the U.S. Department of Health and Human Services of the event.

Contact Information

Should you have any questions regarding this notification or other aspects of the data security event, please contact us at (267) 930-4259.

Very truly yours,

Colin D. Scanlon of
MULLEN COUGHLIN LLC

CDS:bld
Enclosure

EXHIBIT A

General Health System

Return Mail Processing Center
P.O. 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>>

<<Variable Header>>

Dear <<Name 1>>:

General Health System, Inc. ("GHS") writes to notify you of an incident that may have involved some of your personal information. This letter provides details of the incident, our response, and steps you may consider taking to help protect against the possible misuse of your information.

What Happened? On June 28, 2022, GHS became aware of suspicious activity related to certain GHS computer systems. GHS immediately launched an investigation, with the assistance of third-party forensic specialists, to determine the nature and scope of the activity. Through the investigation, it was determined that there was unauthorized access to GHS's network between June 24, 2022 to June 29, 2022. The unauthorized actor had the ability to access certain directories while on the network. Therefore, GHS undertook a diligent and comprehensive review of the contents of the directories determined to be at risk to assess what sensitive information was contained within them and to whom the information related. On October 13, 2022, GHS's review determined that the directories contained certain information related to you.

What Information Was Involved? The following information related to you was present in the directories potentially subject to unauthorized access at the time of the incident: <<Breached Elements>>. Please note we have no evidence to suggest any actual or attempted misuse of this information.

What is GHS Doing? GHS takes the confidentiality, privacy, and security of information in our care very seriously. Upon discovery of the suspicious activity, we immediately commenced an investigation to confirm the nature and scope of the incident and to identify what information could have been affected. We also took steps to enhance our existing security protocols and are evaluating our policies and procedures related to data privacy and security.

GHS arranged to provide you with access to <<CM Length>> months of credit monitoring and identity protection services through Equifax at no cost to you. A description of services and instructions on how to enroll can be found within the enclosed *Steps You Can Take to Help Protect Personal Information*. Please note we are not permitted to enroll you in these services so you must complete the enrollment process yourself.

What You Can Do? We encourage you to remain vigilant against incidents of identity theft and fraud by reviewing your account statements and monitoring your credit reports for any unauthorized or suspicious activity. If you see activity that you did not authorize, contact the credit bureau reporting the activity immediately. We further encourage you to enroll in the complimentary credit monitoring and identity protection services being provided through Equifax.

For More Information. We understand you may have questions about the incident that are not addressed in this letter. If you have questions, please call 855-939-4252 Monday through Friday from 8:00 a.m. to 8:00 p.m. Central Time, excluding holidays. You may also write to GHS at 8595 Picardy Avenue, Suite 100, Baton Rouge, LA 70809. GHS regrets any inconvenience or concern this incident may cause you.

Sincerely,

Edgardo Tenreiro
President and Chief Executive Officer
General Health System, Inc.

Steps You Can Take to Help Protect Personal Information

Credit and Identity Monitoring

Enter your Activation Code: <<*ACTIVATION CODE*>>
Enrollment Deadline: <<Enrollment Deadline>>

Equifax Credit Watch™ Gold

*Note: You must be over age 18 with a credit file to take advantage of the product.

Key Features

- Credit monitoring with email notifications of key changes to your Equifax credit report
- Daily access to your Equifax credit report
- WebScan notifications[1] when your personal information, such as Social Security Number, credit/debit card or bank account numbers are found on fraudulent Internet trading sites
- Automatic fraud alerts[2], which encourages potential lenders to take extra steps to verify your identity before extending credit, plus blocked inquiry alerts and Equifax credit report lock[3]
- Identity Restoration to help restore your identity should you become a victim of identity theft, and a dedicated Identity Restoration Specialist to work on your behalf
- Up to $1,000,000 of identity theft insurance coverage for certain out of pocket expenses resulting from identity theft[4]

Enrollment Instructions

Go to ***www.equifax.com/activate***.
Enter your unique Activation Code of <<*ACTIVATION CODE*>> then click "Submit" and follow these 4 steps:

1. **Register:**
   Complete the form with your contact information and click "Continue".
   If you already have a myEquifax account, click the 'Sign in here' link under the "Let's get started" header. Once you have successfully signed in, you will skip to the Checkout Page in Step 4.
2. **Create Account:**
   Enter your email address, create a password, and accept the terms of use.
3. **Verify Identity:**
   To enroll in your product, we will ask you to complete our identity verification process.
4. **Checkout:**
   Upon successful verification of your identity, you will see the Checkout Page.
   Click 'Sign Me Up' to finish enrolling.

   You're done!
   The confirmation page shows your completed enrollment.
   Click "View My Product" to access the product features.

Monitor Your Accounts

Under U.S. law, a consumer is entitled to one (1) free credit report annually from each of the three (3) major credit reporting bureaus, Equifax, Experian, and TransUnion. To order your free credit report, visit www.annualcreditreport.com or call, toll-free, 1-877-322-8228. You may also directly contact the three major credit reporting bureaus listed below to request a free copy of your credit report.

Consumers have the right to place an initial or extended "fraud alert" on a credit file at no cost. An initial fraud alert is a one (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 (7) years. Should you wish to place a fraud alert on your credit report, please contact any one of the three (3) major credit reporting bureaus listed below.

---

[1] *WebScan searches for your Social Security Number, up to 5 passport numbers, up to 6 bank account numbers, up to 6 credit/debit card numbers, up to 6 email addresses, and up to 10 medical ID numbers. WebScan searches thousands of Internet sites where consumers' personal information is suspected of being bought and sold, and regularly adds new sites to the list of those it searches. However, the Internet addresses of these suspected Internet trading sites are not published and frequently change, so there is no guarantee that we are able to locate and search every possible Internet site where consumers' personal information is at risk of being traded.*

[2] *The Automatic Fraud Alert feature is made available to consumers by Equifax Information Services LLC and fulfilled on its behalf by Equifax Consumer Services LLC.*

[3] *Locking your Equifax credit report will prevent access to it by certain third parties. Locking your Equifax credit report will not prevent access to your credit report at any other credit reporting agency. Entities that may still have access to your Equifax credit report include: companies like Equifax Global Consumer Solutions, which provide you with access to your credit report or credit score, or monitor your credit report as part of a subscription or similar service; companies that provide you with a copy of your credit report or credit score, upon your request; federal, state and local government agencies and courts in certain circumstances; companies using the information in connection with the underwriting of insurance, or for employment, tenant or background screening purposes; companies that have a current account or relationship with you, and collection agencies acting on behalf of those whom you owe; companies that authenticate a consumer's identity for purposes other than granting credit, or for investigating or preventing actual or potential fraud; and companies that wish to make pre-approved offers of credit or insurance to you. To opt out of such pre-approved offers, visit www.optoutprescreen.com.*

[4] *The Identity Theft Insurance benefit is underwritten and administered by American Bankers Insurance Company of Florida, an Assurant company, under group or blanket policies issued to Equifax, Inc., or its respective affiliates for the benefit of its Members. Please refer to the actual policies for terms, conditions, and exclusions of coverage. Coverage may not be available in all jurisdictions.*

As an alternative to a fraud alert, consumers have the right to place a "credit freeze" (also known as a security freeze) on a credit report, free of charge. This will prohibit a credit bureau from releasing information in the credit report without the consumer's express authorization. The credit 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 credit 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 credit freeze on your credit report. To request a security freeze, you will need to provide the following information:

1. Full name (including middle initial as well as Jr., Sr., II, III, etc.);
2. Social Security number;
3. Date of birth;
4. Addresses for the prior two (2) to five (5) 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.); and
7. A copy of either the police report, investigative report, or complaint to a law enforcement agency concerning identity theft if you are a victim of identity theft.

Should you wish to place a fraud alert or credit freeze, please contact the three (3) major credit reporting bureaus listed below. Unlike a fraud alert, you must separately place a credit freeze on your credit file at each credit reporting company.

Equifax	**Experian**	**TransUnion**
https://www.equifax.com/personal/credit-report-services/	https://www.experian.com/help/	https://www.transunion.com/credit-help
1-888-298-0045	1-888-397-3742	1-833-395-6938
Equifax Fraud Alert, P.O. Box 105069 Atlanta, GA 30348-5069	Experian Fraud Alert, P.O. Box 9554, Allen, TX 75013	TransUnion Fraud Alert, P.O. Box 2000, Chester, PA 19016
Equifax Credit Freeze, P.O. Box 105788 Atlanta, GA 30348-5788	Experian Credit Freeze, P.O. Box 9554, Allen, TX 75013	TransUnion Credit Freeze, P.O. Box 160, Woodlyn, PA 19094

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. This notice has not been delayed because of a law enforcement request.

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). 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 also 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 be reported to law enforcement and your state Attorney General.

For District of Columbia residents, the District of Columbia Attorney General may be contacted at: 400 6th Street, NW, Washington, DC 20001; 202-727-3400; and oag.dc.gov.

For Maryland residents, the Maryland Attorney General may be contacted at: 200 St. Paul Place, 16th Floor, Baltimore, MD 21202; 1-410-528-8662 or 1-888-743-0023; and www.oag.state.md.us.

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

For North Carolina residents, the North Carolina Attorney General may be contacted at: 9001 Mail Service Center, Raleigh, NC 27699-9001; 1-877-566-7226 or 1-919-716-6000; and www.ncdoj.gov.