New Hampshire Hospital Association

September 19, 2025

Via Email: DOJ-CPB@doj.nh.gov

Attorney General John M. Formella
Office of the Attorney General
Consumer Protection & Antitrust Bureau
1 Granite Place South
Concord, NH 03301

RE: Notice of Cybersecurity Incident

Dear Attorney General Formella:

I write to notify you on behalf of the New Hampshire Hospital Association ("NHHA"), located at 125 Airport Road, Concord, New Hampshire 03301, about a cybersecurity incident involving two (2) New Hampshire residents that occurred on August 12, 2025. This letter is intended to serve as notice in accordance with NH RSA 359-C:20.

Nature of the Incident

On or about August 12, 2025, an unauthorized person gained access to an NHHA employee's email and business collaboration accounts following the employee's interaction with a phishing email. When the unauthorized access was discovered on August 20, 2025, the incident was elevated to NHHA's response team, the attack was blocked and contained, and NHHA conducted an investigation. At this time, there is no evidence that personally identifiable information ("PII") was viewed by the hacker. However, following a complete scan of the affected accounts, NHHA determined the hacker had access to, and therefore could have viewed, emails containing the names and social security numbers of two (2) New Hampshire residents.

Notice to New Hampshire Residents

On or about September 18, 2025, NHHA provided written notice of this event to the two (2) affected New Hampshire residents in accordance with NH RSA 359-C:20, along with steps the individuals can take to protect themselves. Additionally, NHHA arranged for twelve (12) months of free credit monitoring for the affected individuals. Notice was provided in substantially the form attached hereto as Exhibit A.

Additional Efforts

NHHA is taking steps to improve its security, mitigate cybersecurity risks, and protect against future unauthorized access to its systems. For example, it has implemented additional controls to improve data security generally, it is adjusting its processes to better protect sensitive

data from theft or similar criminal activity in the future, and it is modifying its training for employees to help them better spot future phishing efforts.

Please do not hesitate to contact me if you have any questions regarding this cybersecurity incident.

Sincerely,

Kathy A. Bizarro-Thunberg
Executive Vice President / Federal Relations

(Enclosure)

EXHIBIT A

NOTICE TO AFFECTED INDIVIDUALS

(SEE ATTACHED)

New Hampshire Hospital Association

September 18, 2025

<<First Name>> <<Last Name>>
<<Address 1>>
<<Address 2>>
<<City>>, <<State>> <<Zip>>

RE: Notice of Data Security Incident/Possible Data Breach

Dear <<First Name>> <<Last Name>>:

We write to notify you of an incident in which your personal information may have been exposed to an unauthorized actor who temporarily accessed the email and business collaboration accounts of one of our organization's employees. While, to date, we have no evidence that your information was taken from our systems or has been misused, we provide you with information about the event, our response to it, and resources available to you to help protect your information and identity, should you feel it appropriate to do so. We take seriously the confidentiality of your information and regret any inconvenience this may cause you.

What Happened

On or about August 12, 2025, an employee of our organization opened an email that appeared to contain information transmitted by another employee. In reality, the email was a phishing email. Our employee's interaction with the phishing email resulted in an unauthorized person gaining access to the employee's email and business collaboration accounts for several days before the access was discovered and terminated. When the unauthorized access was discovered, on August 20, 2025, the incident was elevated to our response team, the attack was blocked and contained, and our investigation ensued. Our investigation revealed that the unauthorized actor gained access only to accounts of the above-mentioned employee; they did not get access to or compromise any other systems within our organization. We then examined the affected accounts more carefully to determine if any individuals' personally identifiable information ("PII") was contained in any email or other communication.

During the time that the hacker had access to the affected accounts, the hacker viewed an unknown number of our employee's emails. We do not have information to indicate that the hacker viewed any particular email containing your PII. However, we commissioned a complete scan of the affected accounts to search for PII, as that term is defined under applicable law. You are receiving this communication because your PII was contained in one or more emails in the employee's email account and therefore could have been viewed by the hacker.

At this time, we have no reason to believe that PII was taken by the hacker, but we cannot rule out entirely the possibility that personal information was viewed. Because there is a chance that your information was accessed or viewed, we have opted to provide this notice to you.

What Information Was Involved

You are receiving this letter because our employee's email account contained at least one email that included your name and your social security number.

What We Are Doing

Our investigation has caused us to send this letter to you. We are taking other steps to improve the organization's security, mitigate these types of risks, and protect against further unauthorized access. For example, we have implemented additional controls to improve data security generally. We are adjusting our processes to better protect sensitive data from theft or similar criminal activity in the future. We are also modifying our training for our employees to hopefully spot future phishing efforts.

In addition, we have arranged for twelve months of credit monitoring for you, at no cost to you. Details on how to enroll are included with this letter, along with additional information about the services Equifax will provide if you enroll. We encourage you to do so.

What You Can Do

Again, at this time, there is no evidence that your information has been misused. However, we encourage you to enroll in free credit monitoring offed through Equifax, per the information included with this letter.

In addition to enrolling in the credit monitoring services, we encourage you to remain vigilant against incidents of identity theft and fraud. If you are concerned about the potential implications of this event, there are a number of steps you can take to avoid any adverse impact. Information on additional steps you can take to protect yourself from identity theft can be found at: http://www.consumer.ftc.gov/features/feature-0014-identity-theft. Please review the information contained in the enclosed "Protecting Your Personal Information."

Again, we apologize for any inconvenience this may cause you. Please feel free to call me at <<Telephone Number>> if you have any questions.

Sincerely,

Kathy A. Bizarro-Thunberg
Executive Vice President / Federal Relations

(Enclosure)

Protecting Your Personal Information

We are providing this notice to you so that you can take steps to monitor your credit activity, report any suspicious activity, and take any additional action you believe is necessary. You may consider placing a fraud alert on your credit file, reviewing credit reports for suspicious activity, and reviewing credit card and other financial account information for unauthorized activity.

1. **Website and Enrollment in Credit Monitoring.** Please see the instructions from Equifax that are provided with this letter to enroll.

2. 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. You may also directly contact the three major credit reporting bureaus listed below to request a free copy of your credit report.

If you discover any suspicious items and have enrolled in Equifax credit monitoring offered with this letter, notify them immediately by calling or by logging into the Equifax website and filing a request for help.

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.

3. 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. If you enroll in the offered Equifax credit monitoring, Equifax will place a fraud alert for you. 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. 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	Experian Fraud Reporting	TransUnion Fraud Reporting
1-866-349-5191	1-888-397-3742	1-800-680-7289
P.O. Box 105069	P.O. Box 9554	P.O. Box 2000
Atlanta, GA 30348-5069	Allen, TX 75013	Chester, PA 19022-2000
www.equifax.com	www.experian.com	www.transunion.com

It is necessary to contact only ONE of these bureaus and use only ONE of these methods. If you enroll in the offered Equifax credit monitoring, Equifax will place a fraud alert for you. 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.

4. Security Freeze. As an alternative to a fraud alert, consumers have the right to place a "credit freeze" on a credit report, which will prohibit a credit bureau from releasing information in the credit report without your express authorization. The credit freeze is designed to prevent credit, loans, and services from being approved in your name without your consent. 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. Therefore, 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.

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 to 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.); 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 credit freeze, please contact **each** of the three major credit reporting bureaus above. There is no cost to freeze or unfreeze your credit files.

The credit reporting agencies have three (3) business days after receiving your request to place a security freeze on your credit report. The credit bureaus must also send written confirmation to you within five (5) business days and provide you with a unique personal identification number (PIN) or password, or both, that can be used by you to authorize the removal or lifting of the security freeze. To lift the security freeze in order to allow a specific entity or individual access to your credit report, you must call or send a written request to the credit reporting agencies by mail and include proper identification (name, address and social security number) and the PIN number or password provided to you when you placed the security freeze as well as the identities of those entities or individuals you would like to receive your credit report or the specific period of time you want the credit report available. The credit reporting agencies have three (3) business days after receiving your request to lift the security freeze for those identified entities or for the specified period of time.

To remove the security freeze, you must send a written request to each of the three credit bureaus by mail and include proper identification (name, address, and social security number) and the PIN number or password provided to you when you placed the security freeze. The credit bureaus have three (3) business days after receiving your request to remove the security freeze.

5. You can obtain additional information about the steps you can take to avoid identity theft from the following agencies. You may further educate yourself regarding identity theft, fraud alerts, credit freezes, and the steps you can take to protect your personal information by contacting the consumer reporting bureaus, the Federal Trade Commission, or your state Attorney General. The Federal Trade Commission may be reached at: 600 Pennsylvania Avenue NW, Washington, DC 20580; www.identitytheft.gov; 1-877-ID-THEFT (1-877-438-4338); and 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.

New Hampshire Residents: New Hampshire Department of Justice, Office of the Attorney General, 1 Granite Place South, Concord, NH 03301, www.doj.nh.gov, Telephone: (603) 271-3658.

Maine Residents: Office of the Maine Attorney General, 6 State House Station, Augusta, ME 04333, www.maine.gov/ag, Telephone: 207-626-8800.

New York Residents: Office of the New York State Attorney General, The Capitol, Albany, NY 12224-0341, ag.ny.gov, Telephone: 1-800-771-7755.

EQUIFAX®

<<First Name> <<Last Name>>
Enter your Activation Code: <<Activation Code>>
Enrollment Deadline: <<Date>>

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.

[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.