



Jason Cherry, Partner
Cybersecurity & Data Privacy Team
2029 Century Park East
Los Angeles, CA 90067
Telephone: 207.745.1397

April 21, 2025

VIA U.S. MAIL

Attorney General Mike Hilgers
Office of the Attorney General
Consumer Affairs Response Team
2115 State Capital
Lincoln, NE 68509

Re: Notice of Data Security Incident

To Whom it May Concern:

We represent Onsite Mammography (“Onsite”), located at 815 North Road, Westfield, MA 01085, and are writing to notify your office of an event that may affect the security of certain personal information relating to approximately 36 residents. This notice may be supplemented with any new significant facts learned subsequent to its submission. By providing this notice, Onsite does not waive any rights or defenses regarding the applicability of Nebraska law, the applicability of the Nebraska data event notification statute, or personal jurisdiction.

1. Nature of the Data Event

On or around April 15, 2025, Onsite learned that personal information of certain employees was potentially accessed without authorization. The unauthorized access was the result of a suspicious event Onsite discovered on or about October 4, 2024. Upon discovery, Onsite immediately took steps to address the issue and secure its email environment, including engaging a team of cybersecurity experts, implementing a forced password reset, notifying law enforcement, and launching a comprehensive investigation. The investigation determined that information may have been accessed or acquired without authorization on October 4, 2024. Onsite thereafter undertook a comprehensive review and determined that personal information may have been included. This process was completed on April 15, 2025. Please note that Onsite has no evidence of the misuse, or attempted misuse, of any potentially impacted information.

The information that could have been subject to unauthorized access and/or acquisition includes first and last name, as well as date of birth, Social Security number, medical record number, provider location, procedure information, clinical information, patient account number and provider name.

2. Notice to Nebraska Residents

On or about April 21, 2025, Onsite provided written notice of this event to approximately 36 residents.

3. Other Steps Taken and To Be Taken

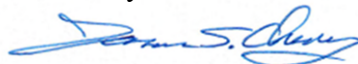
Upon discovering the event, Onsite moved quickly to investigate and respond to the event, assess the security of its network, and identify potentially affected individuals. Onsite is also working to implement additional safeguards and training to its employees.

Additionally, Onsite is providing impacted individuals with guidance on how to better protect against identity theft and fraud, including advising individuals to report any suspected events of identity theft or fraud to their credit card company and/or bank. Onsite is providing individuals with information on how to place a fraud alert and security freeze on one's credit file, information on protecting against tax fraud, the contact details for the national consumer reporting agencies, information on how to obtain a free credit report, a reminder to remain vigilant for events 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.

4. Contact Information

If you have any questions or need additional information, please do not hesitate to contact me at jcherry@constangy.com or 207.745.1397.

Sincerely,

A handwritten signature in blue ink, appearing to read "Jason S. Cherry".

Jason Cherry of
CONSTANGY, BROOKS, SMITH & PROPHETE LLP

Enclosure: Consumer Notification Letter



Secure Processing Center
25 Route 111, P.O. Box 1048
Smithtown, NY 11787

Postal Endorsement Line

<<Full Name>>

<<Address 1>>

<<Address 2>>

<<Address 3>>

<<City>>, <<State>> <<Zip>>

<<Country>>

***Postal IMB Barcode

<<Date>>

Subject: Notice of Data <<Breach or Security Incident>>

Dear <<Full Name>>,

The purpose of this letter is to notify you of a recent data security incident experienced by Onsite Mammography, LLC (“Onsite”), which may have affected your personal and/or protected health information (“PHI”). Onsite takes this incident seriously and is providing you with information about the incident, our response, and steps you can take to help protect your information.

Onsite Mammography is a national service provider that works with health care providers to support imaging services they offer their patients.

What Happened? In October 2024, we discovered unusual activity associated with one employee’s email account. After taking immediate steps to ensure our email environment was secure, we enlisted independent cybersecurity experts to conduct an investigation to determine what happened and whether sensitive information may have been impacted. According to the investigation, an unauthorized actor gained access to the individual’s email account for a brief window of time. Due to the nature of some of the emails in this employee’s inbox, we engaged the services of an outside data analytics vendor, that conducted a comprehensive review of the impacted files to determine whether any PHI was involved. **The investigation further revealed that the actor only had access to the email account and did not have access to any other systems within our network.** The data analytics vendor’s review concluded on February 21, 2025 and revealed that the compromised email included specific health-related information about patients.

What Information Was Involved? The information that may have been impacted in connection with this incident includes your name as well as your <<Data Elements>>. Please note that we have no evidence that any of this information has been misused.

What Are We Doing? As soon as we learned of the incident, we took the measures described above and implemented additional security features to reduce the risk of a similar incident occurring in the future.

We are also offering you the ability to enroll in <<12/24>> months of complimentary Equifax Credit Watch Gold credit monitoring and identity protection services through Epiq, a global technology services leader.

What You Can Do: You can follow the recommendations on the enclosed “Steps You Can Take to Help Protect Your Information” for more information. We also encourage you to enroll in the complimentary monitoring services being offered to you through Equifax by using the enrollment information provided. To enroll in Equifax Credit Watch Gold visit www.equifax.com/activate.

Enter your unique Activation Code: <<Activation Code>>

Enter your Activation Code and click “Submit”.

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.

Please note the deadline to enroll in these complimentary services is <<Enrollment Deadline>>. Please do not discard this letter, as you will need the Activation code provided above to access services.

For More Information: If you have questions or need assistance, please call 855-549-2623. Representatives are available Monday through Friday from 9:00 am – 9:00 pm Eastern Time.

We take this event and the security of information in our care seriously. We regret any concern or inconvenience this incident may cause you.

Sincerely,

Onsite Mammography
815 North Road
Westfield, MA 01085

Steps You Can Take to Help Protect Your Personal Information

Review Your Account Statements and Notify Law Enforcement of Suspicious Activity: As a precautionary measure, we recommend that you remain vigilant by reviewing your account statements and credit reports closely. If you detect any suspicious activity on an account, you should promptly notify the financial institution or company with which the account is maintained. You also should promptly report any fraudulent activity or any suspected incidence of identity theft to proper law enforcement authorities, your state attorney general, and/or the Federal Trade Commission (the "FTC").

Copy of Credit Report: You may obtain a free copy of your credit report from each of the three major credit reporting agencies once every 12 months by visiting www.annualcreditreport.com, calling toll-free 1-877-322-8228, or by completing an Annual Credit Report Request Form and mailing it to Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA 30348. You also can contact one of the following three national credit reporting agencies:

Equifax

P.O. Box 105851
Atlanta, GA 30348
1-800-525-6285
www.equifax.com

Experian

P.O. Box 9532
Allen, TX 75013
1-888-397-3742
www.experian.com

TransUnion

P.O. Box 2000
Chester, PA 19016
1-800-916-8800
www.transunion.com

Fraud Alert: You may want to consider placing a fraud alert on your credit report. An initial fraud alert is free and will stay on your credit file for at least one year. The alert informs creditors of possible fraudulent activity within your report and requests that the creditor contact you prior to establishing any accounts in your name. To place a fraud alert on your credit report, contact any of the three credit reporting agencies identified above. Additional information is available at www.annualcreditreport.com.

Security Freeze: You have the right to put a security freeze on your credit file for up to one year at no cost. This will prevent new credit from being opened in your name without the use of a PIN number that is issued to you when you initiate the freeze. A security freeze is designed to prevent potential creditors from accessing your credit report without your consent. As a result, using a security freeze may interfere with or delay your ability to obtain credit. You must separately place a security freeze on your credit file with each credit reporting agency. In order to place a security freeze, you may be required to provide the consumer reporting agency with information that identifies you including your full name, Social Security number, date of birth, current and previous addresses, a copy of your state-issued identification card, and a recent utility bill, bank statement or insurance statement.

Additional Free Resources: You can obtain information from the consumer reporting agencies, the FTC, or from your respective state Attorney General about fraud alerts, security freezes, and steps you can take toward preventing identity theft. You may report suspected identity theft to local law enforcement, including to the FTC or to the Attorney General in your state.

Federal Trade Commission

600 Pennsylvania Ave, NW
Washington, DC 20580
consumer.ftc.gov
877-438-4338

Maryland Attorney General

200 St. Paul Place
Baltimore, MD 21202
www.marylandattorneygeneral.gov/Pages/CPD
888-743-0023

Oregon Attorney General

1162 Court St., NE
Salem, OR 97301
www.doj.state.or.us/consumer-protec
877-877-9392

California Attorney General

1300 I Street
Sacramento, CA 95814
www.oag.ca.gov/privacy
800-952-5225

New York Attorney General

The Capitol
Albany, NY 12224
800-771-7755
ag.ny.gov

Rhode Island Attorney General

150 South Main Street
Providence, RI 02903
www.riag.ri.gov
401-274-4400

Iowa Attorney General

1305 E. Walnut Street
Des Moines, Iowa 50319
www.iowaattorneygeneral.gov
888-777-4590

Massachusetts Attorney General

Data Privacy and Security Division
Attn: Data Breach Notification
One Ashburton Place
Boston, MA 02108

Washington D.C. Attorney General

400 S 6th Street, NW
Washington, DC 20001
oag.dc.gov/consumer-protection
202-442-9828

Kentucky Attorney General

700 Capitol Avenue, Suite 118
Frankfort, Kentucky 40601
www.ag.ky.gov
502-696-5300

NC Attorney General

9001 Mail Service Center
Raleigh, NC 27699
ncdoj.gov/protectingconsumers/
877-566-7226

You also have certain rights under the Fair Credit Reporting Act (FCRA): These rights include to know what is in your file; to dispute incomplete or inaccurate information; to have consumer reporting agencies correct or delete inaccurate, incomplete, or unverifiable information; as well as other rights. For more information about the FCRA, and your rights pursuant to the FCRA, please visit www.consumer.ftc.gov/sites/default/files/articles/pdf/pdf-0096-fair-credit-reporting-act.pdf.