

Eric Setterlund
Counsel
esetterlund@bradley.com



January 24, 2023

CONFIDENTIAL
VIA OVERNIGHT DELIVERY

Office of the Attorney General
Attn: Security Breach Notification
200 St. Paul Place
Baltimore, MD 21202

Re: Notice of Data Security Incident



To the Office of the Maryland Attorney General:

We are writing on behalf of our client, Outpatient Imaging Affiliates, LLC ("OIA"), to notify you of a data security incident involving OIA, an owner and operator of outpatient imaging facilities. A sample copy of the notification being sent to the 105 affected Maryland residents on January 25, 2023, in accordance with notification requirements under state law is attached to this letter.

OIA recently became aware of suspicious activity in two employees' business email accounts. Upon discovery of this activity on January 4, 2023, OIA immediately took steps to prevent any further unauthorized activity and began an investigation.

Based on the investigation, OIA determined that an unauthorized party gained access via a phishing campaign to two employees' Microsoft365 accounts for one day, between January 3, 2023, and January 4, 2023. Those accounts are separate from OIA's other internal network and systems, which were not involved in the incident. In accessing these accounts, the unauthorized party was able to access an excel spreadsheet on an OIA share point site containing credentialing information for radiologists associated with facilities owned or managed by OIA. There is no indication that the file was exfiltrated (*i.e.*, downloaded) by the unauthorized party, but the information was viewable. Based on the data analysis and address validation efforts that were performed and ultimately completed on January 23, 2023, OIA was able to identify the individuals impacted by this event. The personal information included full name, Social Security number, date of birth, and city of birth.

OIA takes the protection of personal information seriously. OIA was able to quickly identify this incident and take immediate remedial action to prevent any further unauthorized activity, including resetting the employee accounts that were impacted. OIA continues to monitor its systems for any suspicious activity and to review its security controls as appropriate to minimize the risk of any similar event in the future. Finally, OIA continues to educate and remind employees regarding the ongoing risks of phishing campaigns, including simulating such attacks, and OIA will continue

those efforts to increase staff awareness. To date, OIA has not observed any further unauthorized activity on its systems.

OIA has arranged to provide free credit monitoring services for two years to the individuals whose information may have been involved.

If you have any questions regarding this incident or if you desire further information or assistance, please email me at esetterlund@bradley.com or call my direct line at (615) 252-3509.

Sincerely,

A handwritten signature in blue ink, consisting of a stylized 'E' followed by a checkmark-like flourish.

Eric Setterlund

Enclosures



Return Mail Processing
PO Box 999
Suwanee, GA 30024

111*****AUTO**MIXED AADC 300

SAMPLE A. SAMPLE - L01

APT ABC

123 ANY ST

ANYTOWN, US 12345-6789



January 25, 2023

RE: Important Security Notification. Please read this entire letter.

Dear Sample A. Sample:

Outpatient Imaging Affiliates, LLC (“OIA”) values your partnership and respects the privacy of your information, which is why we are writing to inform you of a data security incident that involved your personal information. This letter provides information about the incident and resources available to you.

What happened? OIA recently discovered suspicious activity in two employees’ business email accounts. Upon discovery of this event on January 4, 2023, OIA immediately took steps to prevent any further unauthorized activity and began an investigation. OIA’s investigation determined that an unauthorized party accessed certain Microsoft Outlook business email accounts for one day, between January 3, 2023, and January 4, 2023. Those email accounts are separate from OIA’s other internal network and systems, which were not involved in the incident. Through these accounts, the unauthorized party was able to access a file containing credentialing information for radiologists associated with facilities owned or managed by OIA. We are notifying you because your personal information may have been viewed by the unauthorized party because of this incident.

What information may have been involved? The incident may have involved the disclosure of your name, social security number, date of birth, and city of birth.

What are we doing? OIA takes the protection of your personal information seriously. We were able to quickly identify this incident and take immediate action to prevent any further unauthorized activity. We continue to monitor our systems for any suspicious activity and to review our security controls to minimize the risk of any similar event in the future. To date, we have not observed any further unauthorized activity on our systems. As a precaution, we have arranged for you to receive complimentary identity theft protection and credit monitoring services for a period of two years, at no cost. Please see the attached Reference Guide for enrollment details and instructions on how to enroll.

What can you do? In addition to enrolling in complimentary credit monitoring services, the enclosed Reference Guide includes additional information on general steps you can take to monitor and protect your personal information. We encourage you to remain vigilant against potential identity theft and fraud by carefully reviewing credit reports and account statements to ensure that all activity is valid.

For More Information. We sincerely regret any inconvenience or concern caused by this incident. If you have further questions or concerns, or would like an alternative to enrolling online, please call (833) 256-3152, toll-free Monday through Friday from 8 am – 10 pm Central, or Saturday and Sunday from 10 am – 7 pm Central (excluding major U.S. holidays). Be prepared to provide your engagement number **B084181**.

We regret that this incident occurred and apologize for any inconvenience it may cause you.

Sincerely,

Brandon Odom
Chief Compliance Officer
Outpatient Imaging Affiliates, LLC

Reference Guide

Complimentary Identify Theft Protection Services

To help protect your identity, we are offering **complimentary access to Experian IdentityWorksSM for twenty-four months.**

If you believe there was fraudulent use of your information as a result of this incident and would like to discuss how you may be able to resolve those issues, please reach out to an Experian agent. If, after discussing your situation with an agent, it is determined that identity restoration support is needed, an Experian Identity Restoration agent is available to work with you to investigate and resolve each incident of fraud that occurred from the date of the incident (including, as appropriate, helping you with contacting credit grantors to dispute charges and close accounts; assisting you in placing a freeze on your credit file with the three major credit bureaus; and assisting you with contacting government agencies to help restore your identity to its proper condition).

Please note that Identity Restoration is available to you for 24 months from the date of this letter and does not require any action on your part at this time. The Terms and Conditions for this offer are located at www.ExperianIDWorks.com/restoration.

While identity restoration assistance is **immediately available to you**, we also encourage you to activate the fraud detection tools available through Experian IdentityWorks as a complimentary 24-month membership. This product provides you with superior identity detection and resolution of identity theft. To start monitoring your personal information, please follow the steps below:

- Ensure that you **enroll by April 30, 2023** (Your code will not work after this date.)
- **Visit** the Experian IdentityWorks website to enroll: www.experianidworks.com/credit
- Provide your **activation code: ABCDEFGHI**

If you have questions about the product, need assistance with Identity Restoration that arose as a result of this incident, or would like an alternative to enrolling in Experian IdentityWorks online, please contact Experian's customer care team at (833) 256-3152 by April 30, 2023. Be prepared to provide engagement number **B084181** as proof of eligibility for the Identity Restoration services by Experian.

Additional Details Regarding your 24-month Experian IdentityWorks Membership

A credit card is not required for enrollment in Experian IdentityWorks. You can contact Experian immediately regarding any fraud issues, and have access to the following features once you enroll in Experian IdentityWorks:

- **Experian credit report at signup:** See what information is associated with your credit file. Daily credit reports are available for online members only.*
- **Credit Monitoring:** Actively monitors Experian file for indicators of fraud.
- **Identity Restoration:** Identity Restoration specialists are immediately available to help you address credit and non-credit related fraud.
- **Experian IdentityWorks ExtendCARETM:** You receive the same high-level of Identity Restoration support even after your Experian IdentityWorks membership has expired.
- **\$1 Million Identity Theft Insurance^{**}:** Provides coverage for certain costs and unauthorized electronic fund transfers.

* Offline members will be eligible to call for additional reports quarterly after enrolling.

** The Identity Theft Insurance is underwritten and administered by American Bankers Insurance Company of Florida, an Assurant company. Please refer to the actual policies for terms, conditions, and exclusions of coverage. Coverage may not be available in all jurisdictions.

Monitor Your Accounts

We recommend that you regularly review statements from your accounts and periodically obtain your credit report from one or more of the national credit reporting companies. You may obtain a free copy of your credit report online at www.annualcreditreport.com, by calling toll-free 1-877-322-8228, or by mailing an Annual Credit Report Request Form (available at www.annualcreditreport.com) to Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA, 30348-5281. You may also purchase a copy of your credit report by contacting one or more of the three national credit reporting agencies listed below.

Equifax®
P.O. Box 740241
Atlanta, GA 30374-0241
1-800-685-1111
www.equifax.com

Experian
P.O. Box 9701
Allen, TX 75013-9701
1-888-397-3742
www.experian.com

TransUnion®
P.O. Box 1000
Chester, PA 19016-1000
1-800-888-4213
www.transunion.com

When you receive your credit reports, review them carefully. Look for accounts or creditor inquiries that you did not initiate or do not recognize. Look for information, such as home address and Social Security number that is not accurate. If you see anything you do not understand, call the credit reporting agency at the telephone number on the report.

Place a Fraud Alert on Your Credit File

To protect yourself from possible identity theft, consider placing a fraud alert on your credit file. A fraud alert helps protect against the possibility of an identity thief opening new credit accounts in your name. When a credit grantor checks the credit history of someone applying for credit, the credit grantor gets a notice that the applicant may be the victim of identity theft. The alert notifies the credit grantor to take steps to verify the identity of the applicant. You can request a copy of your credit report, place a fraud alert on your credit report, or call with general inquiries, by calling toll-free any of the three major consumer reporting agencies using the information listed below:

Equifax (888) 766-0008 www.equifax.com P.O. Box 105069 Atlanta, GA 30374	Experian (888) 397-3742 www.experian.com P.O. Box 9554 Allen, TX 75013	TransUnion (800) 680-7289 www.transunion.com P.O. Box 2000 Chester, PA 19016
---	--	--

Requesting a Security Freeze

You have the right to request a security freeze from a consumer reporting agency, free of charge. A security freeze will ensure potential creditors and other third parties are unable to access your credit report without your consent to lift the freeze. The credit reporting agency will issue you a PIN when you initiate a freeze, and your report can only be accessed by providing that PIN. Therefore, using a security freeze may delay your ability to obtain credit.

Unlike a fraud alert, you must separately place a security freeze on your credit report at each credit bureau. To place a security freeze on your credit report you must contact the credit reporting agency by phone, mail, or secure electronic means and follow the agency's instructions.

Below, please find the relevant contact information for the three major consumer reporting agencies to request a security freeze:

Equifax (800) 685-1111 www.equifax.com P.O. Box 105069 Atlanta, GA 30348	Experian (888) 397-3742 www.experian.com P.O. Box 9554 Allen, TX 75013	TransUnion (800) 909-8872 www.transunion.com P.O. Box 2000 Chester, PA 19016
---	--	--

Once you have submitted your request, the credit reporting agency must place the security freeze no later than 1 business day after receiving a request by phone or secure electronic means, and no later than 3 business days after receiving a request by mail. No later than 5 business days after placing the security freeze, the credit reporting agency will send you confirmation and information on how you can remove the freeze in the future.

Contacting the U.S. Federal Trade Commission

You can contact the FTC to learn more about how to protect yourself from becoming a victim of identity theft by using the contact information below:

Federal Trade Commission
Consumer Response Center
600 Pennsylvania Avenue, NW
Washington, DC 20580
1-877-IDTHEFT (438-4338)
www.identitytheft.gov/

For Residents of Maryland

You may also obtain information about preventing and avoiding identity theft from the Maryland Office of the Attorney General:

Maryland Office of the Attorney General
200 St. Paul Place, 25th Floor
Baltimore, MD 21202
Phone: (410) 576-6491
Toll free: (888) 743-0023
Fax: (410) 576-6566
E-mail: idtheft@oag.state.md.us

For Residents of North Carolina

You may also obtain information about preventing and avoiding identity theft from the North Carolina Office of the Attorney General:

North Carolina Office of the Attorney General
Consumer Protection Division
9001 Mail Service Center
Raleigh, NC 27699-9001
Phone: (919)-716-6000
www.ncdoj.gov