MULLEN COUGHLIN LLC
ATTORNEYS AT LAW

Edward J. Finn
Office: (267) 930-4776
Fax: (267) 930-4771
Email: efinn@mullen.law

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

July 22, 2022

VIA U.S. MAIL

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

Re: Supplemental Notice of Data Event

Dear Sir or Madam:

We represent Shields Health Care Group, Inc. ("Shields"), located at 700 Congress St, Suite 204, Quincy, MA 02169, and are writing to supplement Shields' prior notice to your office, attached here as ***Exhibit A.*** Shields' investigation continued and we are notifying your office that the security of certain personal information relating to approximately eight thousand one hundred eighty-one (8,181) New Hampshire residents may have been impacted. The data review is still ongoing, and this notice may be supplemented with a final impacted notice population. By providing this notice, Shields 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 March 28, 2022, Shields was made aware of suspicious activity that may have involved data compromise. Shields immediately launched an investigation into this issue in order to determine the full nature and scope of the event and worked with a number of subject matter specialists to do so. This investigation determined that an unknown actor gained access to certain Shields systems from March 7, 2022 to March 21, 2022. Furthermore, the investigation revealed that certain data was acquired by the unknown actor within this time frame. Although Shields had identified and investigated a security alert on or around March 18, 2022, data theft was not confirmed at that time.

Shields then worked with specialists to perform a comprehensive review of the contents of the affected systems to determine what information was contained in the systems and to whom the information related. This review is ongoing however Shields will be notifying impacted individuals in waves of notice.

The information that could have been subject to unauthorized access includes Social Security number, as well as other protected health information protected under HIPAA.

Notice to New Hampshire Residents

On or about July 25, 2022, Shields will begin to provide written notice of this incident to New Hampshire residents, which includes approximately eight thousand one hundred eighty-one (8,181) residents who potentially have personal information as defined by the New Hampshire statute impacted. Previously, on May 27, 2022, Shields posted website notice and issued media notice pursuant to HIPAA rules. Copies of these notices are attached as ***Exhibit B***. Written notice is being provided in substantially the same form as the letter attached here as ***Exhibit C***. As explained in its prior notice, Shields provides various services for its health care facility partners, which include those found in ***Exhibit B***. These services include management and other services to provider facilities in the MRI, PET/CT, radiation therapy and urgent care space.[1] Shields is providing notifications on behalf of itself and these provider partners as applicable.

Other Steps Taken and To Be Taken

Upon discovering the event, Shields moved quickly to investigate and respond to the incident, assess the security of Shields systems, and identify potentially affected individuals. Further, Shields notified federal law enforcement regarding the event. Shields is also working to implement additional safeguards and training to its employees. Shields is providing access to credit monitoring services for twenty-four (24) months, through Kroll, to individuals whose personal information was potentially affected by this incident, at no cost to these individuals.

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

Shields is providing written notice of this incident to relevant state and federal regulators, as necessary, and to the three major credit reporting agencies, Equifax, Experian, and TransUnion. Shields is also notifying the U.S. Department of Health and Human Services and prominent media pursuant to the Health Insurance Portability and Accountability Act (HIPAA).

[1] The services provided may differ by partner.

Contact Information

Should you have any questions regarding this notification or other aspects of the data security event, please contact us at (267) 930-4776.

Very truly yours,

Edward J. Finn of
MULLEN COUGHLIN LLC

EJF/cob
Enclosure

EXHIBIT A

MULLEN COUGHLIN LLC
ATTORNEYS AT LAW

Edward J. Finn
Office: (267) 930-4776
Fax: (267) 930-4771
Email: efinn@mullen.law

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

June 10, 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 Shields Health Care Group, Inc. ("Shields") located at 700 Congress St, Suite 204, Quincy, MA 02169, and are writing to notify your office of an incident that may affect the security of certain personal information relating to New Hampshire residents. Shields provides management and other services to provider facilities in the MRI, PET/CT, radiation therapy and urgent care space, and is notifying on its behalf and on behalf of its provider partners.[1]

[1] The provider facilities include: Baystate Health Urgent Care, LLC Baystate MRI & Imaging Center, LLC, Brighton Imaging Center, LLC, Cape Cod CT Services, LLC, Cape Cod Imaging Services, LLC (a business associate to Falmouth Hospital Association, Inc), Cape Cod PET/CT Services, LLC, Cape Cod Radiation Therapy Service, LLC, Central Maine Medical Center, Emerson Hospital, Fall River/New Bedford Regional MRI Limited Partnership, Falmouth Hospital Association, Inc., Franklin MRI Center, LLC, Lahey Clinic MRI Services, LLC, Massachusetts Bay MRI Limited Partnership, Mercy Imaging, Inc., MRI/CT of Providence, LLC, Newton-Wellesley MRI Limited Partnership, NW Imaging Management Company, LLC (a business associate to Newton Wellesley Orthopedic Associates, Inc.), Newton-Wellesley Imaging, PC, Newton Wellesley Orthopedic Associates, Inc., Northern MASS MRI Services, Inc., PET-CT Services by Tufts Medical Center and Shields, LLC, Shields and Sports Medicine Atlantic Imaging Management Co, LLC (a business associate SportsMedicine Atlantic Orthopaedics P.A.), Shields CT of Brockton, LLC, Shields Imaging at Anna Jaques Hospital, LLC, Shields Healthcare of Cambridge, Inc., Shields Imaging at University Hospital, LLC, Shields Imaging at York Hospital, LLC, Shields Imaging Management at Emerson Hospital, LLC (a business associate to Emerson Hospital), Shields Imaging of Eastern Mass, LLC, Shields Imaging of Lowell General Hospital, LLC, Shields Imaging of Portsmouth, LLC, Shields Imaging with Central Maine Health, LLC (a business associate to Central Maine Medical Center), Shields Management Company, Inc., Shields MRI & Imaging Center of Cape Cod, LLC, Shields MRI of Framingham, LLC, Shields PET/CT at CMMC, LLC, Shields PET_CT at Berkshire Medical Center, LLC, Shields PET-CT at Cooley Dickinson Hospital, LLC, Shields PET-CT at Emerson Hospital, LLC, Shields Radiology Associates, PC, Shields Signature Imaging, LLC, Shields Sturdy PET-CT, LLC, Shields-Tufts Medical Center Imaging Management, LLC (a business associate to Tufts Medical Center, Inc.), South Shore Regional MRI Limited

The investigation into this matter is ongoing. This notification is preliminary, the data mining process is still ongoing, and this notice will be supplemented with any new significant facts learned subsequent to its submission. By providing this notice, Shields 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 March 28, 2022, Shields was made aware of suspicious activity that may have involved data compromise. Shields immediately launched an investigation into this issue in order to determine the full nature and scope of the event and worked with a number of subject matter specialists to do so.

This investigation determined that an unknown actor gained access to certain Shields systems from March 7, 2022 to March 21, 2022. Furthermore, the investigation revealed that certain data was acquired by the unknown actor within this time frame. Although Shields had identified and investigated a security alert on or around March 18, 2022, data theft was not confirmed at that time.

Shields then worked with specialists to perform a review of the contents of the determined to have been at risk to identify what information was contained therein and to whom the information related. This review is ongoing.

The information that could have been subject to unauthorized access includes Social Security number, as well as other protected health information protected under HIPAA.

Notice to New Hampshire Residents

On or about May 27, 2022, Shields provided substituted notice of this incident to potentially impacted individuals, which includes publication of this incident on Shields' website and media notice. Substitute notice is being provided in substantially the same form as the website and media notices attached here as ***Exhibit A***.

Review and sorting of the impacted data is still ongoing. Shields will send written notice to individuals once the review is complete, and will update your office to confirm the number of New Hampshire residents' whose personal information may be impacted.

Partnership, Southeastern Massachusetts Regional MRI Limited Partnership, SportsMedicine Atlantic Orthopaedics P.A., Tufts Medical Center, Inc., UMass Memorial HealthAlliance MRI Center, LLC, UMass Memorial MRI - Marlborough, LLC, UMass Memorial MRI & Imaging Center, LLC, Winchester Hospital / Shields MRI, LLC, Radiation Therapy of Southeastern Massachusetts, LLC, Radiation Therapy of Winchester, LLC, South Suburban, Oncology Center Limited Partnership, Shields Imaging of North Shore, LLC

Other Steps Taken and To Be Taken

Upon discovering the event, Shields moved quickly to investigate and respond to the incident, assess the security of Shields systems, and notify potentially affected individuals. In order to promptly alert potentially impacted individuals, Shields provided substitute and media notice

Additionally, Shields will be providing impacted individuals with guidance on how to better protect against identity theft and fraud, including advising individuals to report any suspected incidents of identity theft or fraud to their credit card company and/or bank. Shields will provide 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. Shields will be providing credit monitoring and identity restoration services with written notice to individuals.

Shields provided written notice to the U.S. Department of Health and Human Services and prominent media pursuant to the Health Insurance Portability and Accountability Act (HIPAA).

Contact Information

Should you have any questions regarding this notification or other aspects of the data security event, please contact us at (267) 930-4776.

Very truly yours,

Edward J. Finn of
MULLEN COUGHLIN LLC

EJF/tmr
Enclosure

https://shields.com/

Search...

Shields Healthcare Group - ...

Notice of Data Security Incident

Shields HEALTH CARE GROUP

Shields Express Link | Patients | Company | News | Contact

Search

Select Language

WHY SHIELDS | PARTNER WITH US | OUR SERVICES | FIND A LOCATION | EMPLOYMENT

Where is your next career opportunity?

The door is open at Shields.

Learn more

SHIELDS **EXPRESS LINK**

Online access to reports and images

3:58 PM
5/27/2022

EXHIBIT A

June 10, 2022

Notice of Data Security Incident

Shields Health Care Group, Inc. ("Shields") recently became aware of suspicious activity on its network. Shields provides management and imaging services on behalf of the health care facilities ("Facility Partners") listed below. With the assistance of third-party forensic specialists, we took immediate steps to contain the incident and to investigate the nature and scope of the incident. Shields is issuing this notice on behalf of itself and the Facility Partners to communicate what is known about the incident, our response, and steps impacted individuals can take, if deemed appropriate. Certain patients of these Facility Partners may be impacted.

What Happened? On March 28, 2022, Shields was alerted to suspicious activity that may have involved data compromise. Shields immediately launched an investigation into this issue and worked with subject matter specialists to determine the full nature and scope of the event.

This investigation determined that an unknown actor gained access to certain Shields systems from March 7, 2022 to March 21, 2022. Furthermore, the investigation revealed that certain data was acquired by the unknown actor within that time frame. Although Shields had identified and investigated a security alert on or around March 18, 2022, data theft was not confirmed at that time.

What Information Was Involved? To date, we have no evidence to indicate that any information from this incident was used to commit identity theft or fraud. However, the type of information that was or may have been impacted could include one or more of the following: Full name, Social Security number, date of birth, home address, provider information, diagnosis, billing information, insurance number and information, medical record number, patient ID, and other medical or treatment information. Shields review of the impacted data is ongoing.

What Information Was Involved? To date, we have no evidence to indicate that any information from this incident was used to commit identity theft or fraud. However, the type of information that was or may have been impacted could include one or more of the following: Full name, Social Security number, date of birth, home address, provider information, diagnosis, billing information, insurance number and information, medical record number, patient ID, and other medical or treatment information. Shields review of the impacted data is ongoing.

What Are We Doing? Shields takes the confidentiality, privacy, and security of information in our care seriously. Upon discovery, we took steps to secure our systems, including rebuilding certain systems, and conducted a thorough investigation to confirm the nature and scope of the activity and to determine who may be affected. Additionally, while we have safeguards in place to protect data in our care, we continue to review and further enhance these protections as part of our ongoing commitment to data security.

We have notified federal law enforcement, and will be reporting this incident to relevant state and federal regulators. Further, once we complete the review of the impacted data, we will directly notify impacted individuals where possible so that they may take further steps to help protect their information, should they feel it is appropriate to do so.

What Can Affected Individuals Do? While we have no evidence to indicate identity theft or fraud occurred as a result of this incident, we encourage impacted individuals to review ***Steps You Can Take to Help Protect Your Information***, which is included below.

For More Information. We understand you may have additional questions concerning this incident. Individuals can direct questions to (855) 503-3386. The call center hours will be 8:00am-5:30pm Central Time, Monday through Friday, excluding major U.S. holidays.

Steps You Can Take to Help Protect Your Information

Monitor Your Accounts

-

Under U.S. law, a consumer is entitled to one free credit report annually from each of the three 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.

Under U.S. law, a consumer is entitled to one free credit report annually from each of the three 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 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. Should you wish to place a fraud alert, please contact any one of the three major credit reporting bureaus listed below.

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 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 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, 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 the three major credit reporting bureaus listed below:

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

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 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. This notice has not been delayed by law enforcement.

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 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. 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 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 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. 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.

For Rhode Island residents, the Rhode Island Attorney General may be reached at: 150 South Main Street, Providence, RI 02903; www.riag.ri.gov; and 1-401-274-4400. The number of Rhode Island residents impacted is not currently confirmed. Under Rhode Island law, you have the right to obtain any police report filed in regard to this incident.

Facility Partners

***Facilities / Entity**
Baystate Health Urgent Care, LLC
Baystate MRI & Imaging Center, LLC
Brighton Imaging Center, LLC
Cape Cod CT Services, LLC
Cape Cod Imaging Services, LLC (a business associate to Falmouth Hospital Association, Inc)
Cape Cod PET/CT Services, LLC
Cape Cod Radiation Therapy Service, LLC

Facility Partners

***Facilities / Entity**

Baystate Health Urgent Care, LLC
Baystate MRI & Imaging Center, LLC
Brighton Imaging Center, LLC
Cape Cod CT Services, LLC
Cape Cod Imaging Services, LLC (a business associate to Falmouth Hospital Association, Inc)
Cape Cod PET/CT Services, LLC
Cape Cod Radiation Therapy Service, LLC
Central Maine Medical Center
Emerson Hospital
Fall River/New Bedford Regional MRI Limited Partnership
Falmouth Hospital Association, Inc.
Franklin MRI Center, LLC
Lahey Clinic MRI Services, LLC
Massachusetts Bay MRI Limited Partnership
Mercy Imaging, Inc.
MRI/CT of Providence, LLC
Newton-Wellesley MRI Limited Partnership
NW Imaging Management Company, LLC (a business associate to Newton Wellesley Orthopedic Associates, Inc.)
Newton-Wellesley Imaging, PC
Newton Wellesley Orthopedic Associates, Inc.
Northern MASS MRI Services, Inc.
PET-CT Services by Tufts Medical Center and Shields, LLC
Shields and Sports Medicine Atlantic Imaging Management Co, LLC (a business associate SportsMedicine Atlantic Orthopaedics P.A.)
Shields CT of Brockton, LLC
Shields Imaging at Anna Jaques Hospital, LLC
Shields Healthcare of Cambridge, Inc.
Shields Imaging at University Hospital, LLC
Shields Imaging at York Hospital, LLC
Shields Imaging Management at Emerson Hospital, LLC (a business associate to Emerson Hospital)
Shields Imaging of Eastern Mass, LLC
Shields Imaging of Lowell General Hospital, LLC
Shields Imaging of Portsmouth, LLC
Shields Imaging with Central Maine Health, LLC (a business associate to Central Maine Medical Center)
Shields Management Company, Inc.
Shields MRI & Imaging Center of Cape Cod, LLC
Shields MRI of Framingham, LLC
Shields PET/CT at CMMC, LLC
Shields PET_CT at Berkshire Medical Center, LLC
Shields PET-CT at Cooley Dickinson Hospital, LLC

Shields Imaging at University Hospital, LLC
Shields Imaging at York Hospital, LLC
Shields Imaging Management at Emerson Hospital, LLC (a business associate to Emerson Hospital)
Shields Imaging of Eastern Mass, LLC
Shields Imaging of Lowell General Hospital, LLC
Shields Imaging of Portsmouth, LLC
Shields Imaging with Central Maine Health, LLC (a business associate to Central Maine Medical Center)
Shields Management Company, Inc.
Shields MRI & Imaging Center of Cape Cod, LLC
Shields MRI of Framingham, LLC
Shields PET/CT at CMMC, LLC
Shields PET_CT at Berkshire Medical Center, LLC
Shields PET-CT at Cooley Dickinson Hospital, LLC
Shields PET-CT at Emerson Hospital, LLC
Shields Radiology Associates, PC
Shields Signature Imaging, LLC
Shields Sturdy PET-CT, LLC
Shields-Tufts Medical Center Imaging Management, LLC (a business associate to Tufts Medical Center, Inc.)
South Shore Regional MRI Limited Partnership
Southeastern Massachusetts Regional MRI Limited Partnership
SportsMedicine Atlantic Orthopaedics P.A.
Tufts Medical Center, Inc.
UMass Memorial HealthAlliance MRI Center, LLC
UMass Memorial MRI – Marlborough, LLC
UMass Memorial MRI & Imaging Center, LLC
Winchester Hospital / Shields MRI, LLC
Radiation Therapy of Southeastern Massachusetts, LLC
Radiation Therapy of Winchester, LLC
South Suburban Oncology Center Limited Partnership
Shields Imaging of North Shore, LLC

MEDIA NOTICE

Shields Health Care Group Notification of Data Privacy Event

Shields Health Care Group ("Shields") recently became aware of suspicious activity on its network. Shields provides management and imaging services on behalf of the health care facilities ("Facility Partners") listed below. With the assistance of third-party forensic specialists, Shields took immediate steps to contain the incident and to investigate the nature and scope of the incident. Shields is issuing this notice on behalf of itself and the Facility Partners to communicate what is known about the incident, the response, and steps impacted individuals can take, if deemed appropriate. Certain patients of these Facility Partners may be impacted.

What Happened? On March 28, 2022, Shields was alerted to suspicious activity that may have involved data compromise. Shields immediately launched an investigation into this issue and worked with subject matter specialists to determine the full nature and scope of the event.

This investigation determined that an unknown actor gained access to certain Shields systems from March 7, 2022 to March 21, 2022. Furthermore, the investigation revealed that certain data was acquired by the unknown actor within that time frame. Although Shields had identified and investigated a security alert on or around March 18, 2022, data theft was not confirmed at that time.

What Information Was Involved? To date, Shields has no evidence to indicate that any information from this incident was used to commit identity theft or fraud. However, the type of information that was or may have been impacted could include one or more of the following: Full name, Social Security number, date of birth, home address, provider information, diagnosis, billing information, insurance number and information, medical record number, patient ID, and other medical or treatment information. Shields review of the impacted data is ongoing.

What Are We Doing? Shields takes the confidentiality, privacy, and security of information in its care seriously. Upon discovery, Shields secured its system and launched an investigation with third party forensics specialists to determine the nature of the activity and the scope of potentially impacted data. Shields rebuilt certain systems and continues to review and further enhance its existing protections as part of an ongoing commitment to data security.

Shields notified federal law enforcement and will report this incident to relevant state and federal regulators. Once the review of impacted data is complete, Shields will directly notify impacted individuals where possible so that they may take further steps to help protect their information, should they feel it appropriate to do so.

What Can Affected Individuals Do? While Shields has no evidence to indicate identity theft or fraud occurred as a result of this incident, Shields encourages impacted individuals to review *Steps You Can Take to Help Protect Your Information*, which is included below.

For More Information. Individuals with questions about this event can call (855) 503-3386 from 9:00 a.m. to 6:30 p.m., Eastern Time, Monday through Friday, excluding major U.S. holidays. Individuals can also find information on our website, at https://shields.com/.

Steps Individuals Can Take to Help Protect Their Information

Monitor Your Accounts

Under U.S. law, a consumer is entitled to one free credit report annually from each of the three 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 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. Should you wish to place a fraud alert, please contact any one of the three major credit reporting bureaus listed below.

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 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 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, 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 the three major credit reporting bureaus listed below:

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 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. This notice has not been delayed by law enforcement.

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 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. 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.

For Rhode Island residents, the Rhode Island Attorney General may be reached at: 150 South Main Street, Providence, RI 02903; www.riag.ri.gov; and 1-401-274-4400. The number of impacted Rhode Island residents is unknown at this time. Under Rhode Island law, you have the right to obtain any police report filed in regard to this incident.

Facility Partners

***Facilities / Entity**
Baystate Health Urgent Care, LLC
Baystate MRI & Imaging Center, LLC
Brighton Imaging Center, LLC
Cape Cod CT Services, LLC
Cape Cod Imaging Services, LLC (a business associate to Falmouth Hospital Association, Inc)
Cape Cod PET/CT Services, LLC
Cape Cod Radiation Therapy Service, LLC
Central Maine Medical Center
Emerson Hospital
Fall River/New Bedford Regional MRI Limited Partnership
Falmouth Hospital Association, Inc.
Franklin MRI Center, LLC
Lahey Clinic MRI Services, LLC
Massachusetts Bay MRI Limited Partnership
Mercy Imaging, Inc.
MRI/CT of Providence, LLC
Newton-Wellesley MRI Limited Partnership
NW Imaging Management Company, LLC (a business associate to Newton Wellesley Orthopedic Associates, Inc.)
Newton-Wellesley Imaging, PC
Newton Wellesley Orthopedic Associates, Inc.
Northern MASS MRI Services, Inc.
PET-CT Services by Tufts Medical Center and Shields, LLC
Shields and Sports Medicine Atlantic Imaging Management Co, LLC (a business associate SportsMedicine Atlantic Orthopaedics P.A.)
Shields CT of Brockton, LLC
Shields Imaging at Anna Jaques Hospital, LLC
Shields Healthcare of Cambridge, Inc.
Shields Imaging at University Hospital, LLC
Shields Imaging at York Hospital, LLC
Shields Imaging Management at Emerson Hospital, LLC (a business associate to Emerson Hospital)
Shields Imaging of Eastern Mass, LLC
Shields Imaging of Lowell General Hospital, LLC
Shields Imaging of Portsmouth, LLC
Shields Imaging with Central Maine Health, LLC (a business associate to Central Maine Medical Center)
Shields Management Company, Inc.
Shields MRI & Imaging Center of Cape Cod, LLC

Shields MRI of Framingham, LLC
Shields PET/CT at CMMC, LLC
Shields PET_CT at Berkshire Medical Center, LLC
Shields PET-CT at Cooley Dickinson Hospital, LLC
Shields PET-CT at Emerson Hospital, LLC
Shields Radiology Associates, PC
Shields Signature Imaging, LLC
Shields Sturdy PET-CT, LLC
Shields-Tufts Medical Center Imaging Management, LLC (a business associate to Tufts Medical Center, Inc.)
South Shore Regional MRI Limited Partnership
Southeastern Massachusetts Regional MRI Limited Partnership
SportsMedicine Atlantic Orthopaedics P.A.
Tufts Medical Center, Inc.
UMass Memorial HealthAlliance MRI Center, LLC
UMass Memorial MRI - Marlborough, LLC
UMass Memorial MRI & Imaging Center, LLC
Winchester Hospital / Shields MRI, LLC
Radiation Therapy of Southeastern Massachusetts, LLC
Radiation Therapy of Winchester, LLC
South Suburban Oncology Center Limited Partnership
Shields Imaging of North Shore, LLC

EXHIBIT B

WEBSITE NOTICE – Shields Health Care Group

Shields Health Care Group, Inc. ("Shields") recently became aware of suspicious activity on its network. Shields provides management and imaging services on behalf of the health care facilities ("Facility Partners") listed below. With the assistance of third-party forensic specialists, we took immediate steps to contain the incident and to investigate the nature and scope of the incident. Shields is issuing this notice on behalf of itself and the Facility Partners to communicate what is known about the incident, our response, and steps impacted individuals can take, if deemed appropriate. Certain patients of these Facility Partners may be impacted.

What Happened? On March 28, 2022, Shields was alerted to suspicious activity that may have involved data compromise. Shields immediately launched an investigation into this issue and worked with subject matter specialists to determine the full nature and scope of the event.

This investigation determined that an unknown actor gained access to certain Shields systems from March 7, 2022 to March 21, 2022. Furthermore, the investigation revealed that certain data was acquired by the unknown actor within that time frame. Although Shields had identified and investigated a security alert on or around March 18, 2022, data theft was not confirmed at that time.

Shields worked with specialists to perform a comprehensive review of the potentially affected data to determine what individual personal information may have been involved, and began notifying its health care facility partners on May 25, 2022. While Shields' review is still ongoing, Shields is providing notice to individuals identified thus far as being impacted.

What Information Was Involved? The type of information that was or may have been impacted could include one or more of the following: full name, Social Security number, date of birth, home address, provider information, diagnosis, billing information, insurance number and information, medical record number, patient ID, and other medical or treatment information.

What Are We Doing? Shields takes the confidentiality, privacy, and security of information in our care seriously. Upon discovery, we took steps to secure our systems, including rebuilding certain systems, and conducted a thorough investigation to confirm the nature and scope of the activity and to determine who may be affected. Additionally, while we have safeguards in place to protect data in our care, we continue to review and further enhance these protections as part of our ongoing commitment to data security.

We have notified federal law enforcement, and will be reporting this incident to relevant state and federal regulators. Further, once we complete the review of the impacted data, we will directly notify impacted individuals where possible so that they may take further steps to help protect their information, should they feel it is appropriate to do so.

What Can Affected Individuals Do? We encourage impacted individuals to review *Steps You Can Take to Help Protect Your Information*, which is included below.

For More Information. We understand you may have additional questions concerning this incident. Individuals can direct questions to (855) 503-3386. The call center hours will be 8:00 am-5:30 pm Central Time, Monday through Friday, excluding major U.S. holidays.

Steps You Can Take to Help Protect Your Information

Monitor Your Accounts

Under U.S. law, a consumer is entitled to one free credit report annually from each of the three 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 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. Should you wish to place a fraud alert, please contact any one of the three major credit reporting bureaus listed below.

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 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 credit 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, 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 the three major credit reporting bureaus listed below:

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 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. This notice has not been delayed by law enforcement.

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 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. 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.

For Rhode Island residents, the Rhode Island Attorney General may be reached at: 150 South Main Street, Providence, RI 02903; www.riag.ri.gov; and 1-401-274-4400. The number of Rhode Island residents impacted is not currently confirmed. Under Rhode Island law, you have the right to obtain any police report filed in regard to this incident.

Facility Partners

***Facilities / Entity**
Baystate Health Urgent Care, LLC
Baystate MRI & Imaging Center, LLC
Brighton Imaging Center, LLC
Cape Cod CT Services, LLC
Cape Cod Imaging Services, LLC (a business associate to Falmouth Hospital Association, Inc)
Cape Cod PET/CT Services, LLC
Cape Cod Radiation Therapy Service, LLC
Central Maine Medical Center
Emerson Hospital
Fall River/New Bedford Regional MRI Limited Partnership
Falmouth Hospital Association, Inc.
Franklin MRI Center, LLC
Lahey Clinic MRI Services, LLC
Massachusetts Bay MRI Limited Partnership
Mercy Imaging, Inc.
MRI/CT of Providence, LLC
Newton-Wellesley MRI Limited Partnership
NW Imaging Management Company, LLC (a business associate to Newton Wellesley Orthopedic Associates, Inc.)
Newton-Wellesley Imaging, PC
Newton Wellesley Orthopedic Associates, Inc.
Northern MASS MRI Services, Inc.
PET-CT Services by Tufts Medical Center and Shields, LLC
Shields and Sports Medicine Atlantic Imaging Management Co, LLC (a business associate SportsMedicine Atlantic Orthopaedics P.A.)
Shields CT of Brockton, LLC
Shields Imaging at Anna Jaques Hospital, LLC
Shields Healthcare of Cambridge, Inc.
Shields Imaging at University Hospital, LLC
Shields Imaging at York Hospital, LLC
Shields Imaging Management at Emerson Hospital, LLC (a business associate to Emerson Hospital)
Shields Imaging of Eastern Mass, LLC
Shields Imaging of Lowell General Hospital, LLC
Shields Imaging of Portsmouth, LLC
Shields Imaging with Central Maine Health, LLC (a business associate to Central Maine Medical Center)
Shields Management Company, Inc.
Shields MRI & Imaging Center of Cape Cod, LLC
Shields MRI of Framingham, LLC

Shields PET/CT at CMMC, LLC
Shields PET_CT at Berkshire Medical Center, LLC
Shields PET-CT at Cooley Dickinson Hospital, LLC
Shields PET-CT at Emerson Hospital, LLC
Shields Radiology Associates, PC
Shields Signature Imaging, LLC
Shields Sturdy PET-CT, LLC
Shields-Tufts Medical Center Imaging Management, LLC (a business associate to Tufts Medical Center, Inc.)
South Shore Regional MRI Limited Partnership
Southeastern Massachusetts Regional MRI Limited Partnership
SportsMedicine Atlantic Orthopaedics P.A.
Tufts Medical Center, Inc.
UMass Memorial HealthAlliance MRI Center, LLC
UMass Memorial MRI - Marlborough, LLC
UMass Memorial MRI & Imaging Center, LLC
Winchester Hospital / Shields MRI, LLC
Radiation Therapy of Southeastern Massachusetts, LLC
Radiation Therapy of Winchester, LLC
South Suburban Oncology Center Limited Partnership
Shields Imaging of North Shore, LLC

MEDIA NOTICE

Shields Health Care Group Notification of Data Privacy Event

Shields Health Care Group ("Shields") recently became aware of suspicious activity on its network. Shields provides management and imaging services on behalf of the health care facilities ("Facility Partners")[1]. With the assistance of third-party forensic specialists, Shields took immediate steps to contain the incident and to investigate the nature and scope of the incident. Shields is issuing this notice on behalf of itself and the Facility Partners to communicate what is known about the incident, the response, and steps impacted individuals can take, if deemed appropriate. Certain patients of these Facility Partners may be impacted.

What Happened? On March 28, 2022, Shields was alerted to suspicious activity that may have involved data compromise. Shields immediately launched an investigation into this issue and worked with subject matter specialists to determine the full nature and scope of the event.

This investigation determined that an unknown actor gained access to certain Shields systems from March 7, 2022 to March 21, 2022. Furthermore, the investigation revealed that certain data was acquired by the unknown actor within that time frame. Although Shields had identified and investigated a security alert on or around March 18, 2022, data theft was not confirmed at that time.

Shields worked with specialists to perform a comprehensive review of the potentially affected data to determine what individual personal information may have been involved, and began notifying its health care facility partners on May 25, 2022. While Shields' review is still ongoing, Shields is providing notice to individuals identified thus far as being impacted.

What Information Was Involved? The type of information that was or may have been impacted could include one or more of the following: full name, Social Security number, date of birth, home address, provider information, diagnosis, billing information, insurance number and information, medical record number, patient ID, and other medical or treatment information. Shields review of the impacted data is ongoing.

What Are We Doing? Shields takes the confidentiality, privacy, and security of information in its care seriously. Upon discovery, Shields secured its system and launched an investigation with third party forensics specialists to determine the nature of the activity and the scope of potentially impacted data. Shields rebuilt certain systems and continues to review and further enhance its existing protections as part of an ongoing commitment to data security.

Shields notified federal law enforcement and will report this incident to relevant state and federal regulators. Once the review of impacted data is complete, Shields will directly notify impacted individuals where possible so that they may take further steps to help protect their information, should they feel it appropriate to do so.

What Can Affected Individuals Do? Shields encourages impacted individuals to review *Steps Individuals Can Take to Help Protect Their Information*, which is included below.

For More Information. Individuals with questions about this event can call (855) 503-3386 from 9:00 a.m. to 6:30 p.m., Eastern Time, Monday through Friday, excluding major U.S. holidays. Individuals can also find information on our website, at https://shields.com/.

---

[1] Services may differ by partner. A list of Facilities Partners can be found here: https://shields.com/notice-of-data-security-incident/

Steps Individuals Can Take to Help Protect Their Information

Monitor Your Accounts

Under U.S. law, a consumer is entitled to one free credit report annually from each of the three 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 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. Should you wish to place a fraud alert, please contact any one of the three major credit reporting bureaus listed below.

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 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 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, 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 the three major credit reporting bureaus listed below:

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 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. This notice has not been delayed by law enforcement.

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 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. 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.

For Rhode Island residents, the Rhode Island Attorney General may be reached at: 150 South Main Street, Providence, RI 02903; www.riag.ri.gov; and 1-401-274-4400. The number of impacted Rhode Island residents is unknown at this time. Under Rhode Island law, you have the right to obtain any police report filed in regard to this incident.

EXHIBIT C

<<Date>> (Format: Month Day, Year)

<<first_name>> <<middle_name>> <<last_name>> <<suffix>>
<<address_1>>
<<address_2>>
<<city>>, <<state_province>> <<postal_code>>
<<country>>

Notice of Security Incident

Dear <<first_name>> <<middle_name>> <<last_name>> <<suffix>>:

Shields Health Care Group, Inc. ("Shields") is writing to inform you of a recent data security event that <<b2b_text_1(involves/may involve)>> some of your information. Shields provides management and imaging services on behalf of health care facilities, including: <<b2b_text_2(Facility Name)>>.[1] We are providing information about the event, our response, and steps to help protect against the possibility of identity theft and fraud, should you find it is necessary to do so.

What Happened? On March 28, 2022, Shields was alerted to suspicious activity potentially involving data compromise. Shields initiated our incident response protocols and immediately launched an investigation with third-party forensics specialists to determine the nature of the activity and the scope of potentially impacted data.

The investigation determined an unknown actor gained access to certain Shields systems from March 7, 2022, to March 21, 2022. Furthermore, the investigation revealed certain data was acquired by the unknown actor within that time frame. Although Shields had identified and investigated a security alert on or around March 18, 2022, data theft was not confirmed at that time.

We worked with specialists to perform a comprehensive review of the potentially affected data to determine what information may have been impacted, and began notifying our health care facility partners on May 25, 2022. While our review is still ongoing, we are providing notice to individuals identified thus far as being impacted.

What Information Was Involved? We determined the impacted information may include: <<b2b_text_3(data elements)>> <<b2b_text_4(data elements cont.)>>.

What We Are Doing. We take this incident, and the security of information held on our systems, very seriously. Upon discovery, we immediately activated our incident response protocols, notified law enforcement, and launched an investigation to confirm the nature of the activity and the scope of potentially impacted data. We also rebuilt certain systems on our network. While we have safeguards in place to protect our data, we are working to review and enhance these protections as part of our ongoing commitment to data security. We are also offering you free identity monitoring services for twenty-four (24) months through Kroll.

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 suspicious activity or errors. You may also review the information contained in the attached "Steps You Can Take to Help Protect Your Personal Information." There you will also find more information on the identity monitoring services we are making available to you. While Shields will cover the cost of these services, you will need to complete the activation process. Additional information describing your services is included with this letter.

[1] More information can be found here: https://shields.com/notice-of-data-security-incident/.

For More Information. If you have additional questions, please call our dedicated assistance line at 855-503-3386, Monday through Friday, 9:00 am to 6:30 pm Eastern Time (except U.S. holidays). You may also write to Shields at Crown Colony Park, 700 Congress Street, Suite 204, Quincy, MA 02169.

We apologize for any inconvenience or concern this event may cause.

Sincerely,

Peter Ferrari
President
Shields Health Care Group, Inc.

Steps You Can Take to Help Protect Your Personal Information

Activate Identity Monitoring

To help relieve concerns and restore confidence following this incident, we have secured the services of Kroll to provide identity monitoring at no cost to you for twenty-four (24) months. Kroll is a global leader in risk mitigation and response, and their team has extensive experience helping people who have sustained an unintentional exposure of confidential data. Your identity monitoring services include Credit Monitoring, Fraud Consultation, and Identity Theft Restoration.[2]

Visit **https://enroll.krollmonitoring.com** to activate and take advantage of your identity monitoring services.
You have until <<b2b_text_6(activation deadline)>> to activate your identity monitoring services.
Membership Number: **<<Membership Number s_n>>**

For more information about Kroll and your Identity Monitoring services, you can visit info.krollmonitoring.com.

You have been provided with access to the following services from Kroll:

Single Bureau Credit Monitoring
You will receive alerts when there are changes to your credit data—for instance, when a new line of credit is applied for in your name. If you do not recognize the activity, you'll have the option to call a Kroll fraud specialist, who will be able to help you determine if it is an indicator of identity theft.

Fraud Consultation
You have unlimited access to consultation with a Kroll fraud specialist. Support includes showing you the most effective ways to protect your identity, explaining your rights and protections under the law, assistance with fraud alerts, and interpreting how personal information is accessed and used, including investigating suspicious activity that could be tied to an identity theft event.

Identity Theft Restoration
If you become a victim of identity theft, an experienced Kroll licensed investigator will work on your behalf to resolve related issues. You will have access to a dedicated investigator who understands your issues and can do most of the work for you. Your investigator will be able to dig deep to uncover the scope of the identity theft, and then work to resolve it.

Monitor Your Accounts

Under U.S. law, a consumer is entitled to one free credit report annually from each of the three 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 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. Should you wish to place a fraud alert, please contact any one of the three major credit reporting bureaus listed below.

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 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/security freeze on your credit report. To request a security freeze, you may need to provide the following information, depending on whether you make the request online, by phone, or by mail:

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. Social Security Card, pay stub, or W2;

[2] Kroll's activation website is only compatible with the current version or one version earlier of Chrome, Firefox, Safari and Edge. To receive credit services, you must be over the age of 18 and have established credit in the U.S., have a Social Security number in your name, and have a U.S. residential address associated with your credit file.

7. A legible photocopy of a government-issued identification card (state driver's license or ID card, etc.); and
8. 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 or fraud alert, please contact the three major credit reporting bureaus listed below:

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 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. Further, you have the right to obtain any police report filed in regard to this incident. This notice has not been delayed by law enforcement.

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 Massachusetts Residents, under Massachusetts law, you have the right to obtain a police report in regard to this incident. If you are the victim of identity theft, you also have the right to file a police report and obtain a copy of it.

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 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. 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.

For Rhode Island residents, the Rhode Island Attorney General may be reached at: 150 South Main Street, Providence, RI 02903; www.riag.ri.gov; and 1-401-274-4400. Under Rhode Island law, 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.