24652

ROCKEFELLER ARCHIVE CENTER
Mail Processing Center
PO Box 509
Buford, GA 30515

December 6, 2021

[redacted]

Re: Notice Data Breach

Dear [redacted],

Please read this letter in its entirety.

We are sending this letter to notify you that we experienced a data incident that may have involved your personal information. Unfortunately, Massachusetts regulations prohibit us from disclosing information on the incident in this notification letter. However, details are available through our call center helpline or through us, as described below.

What is the Rockefeller Archive Center doing to address this situation?

The attached sheet describes steps you can take to protect your identity and personal information. In addition, we would like to offer you access to the following:

- Single Bureau Credit Monitoring services at no charge. These services provide you with alerts for twenty-four months from the date of enrollment when changes occur to your credit report.
- In addition, we are offering identity theft protection services through First Watch Technologies ("FWT"). FWT identity protection services include: 24 months of credit monitoring, a $1,000,000 insurance reimbursement policy, and fully managed id theft recovery services. With this protection, FWT will help you resolve issues if your identity is compromised.
- We encourage you to contact FWT with any questions and to enroll in free identity protection services by calling 866-346-4863 and using the Enrollment Code provided below. FWT representatives are available Monday through Friday from 9 am – 5:30 pm eastern. When prompted, please provide the following unique code to receive services: [redacted]. Please note the deadline to enroll is **March 6, 2022**

Again, at this time, there is no evidence that personal information has been misused. However, we encourage you to take full advantage of this service offering. FWT representatives have been fully versed on the incident and can answer questions concerns you may have regarding protection of personal information. To extend these services, enrollment in the monitoring services is required.

What can I do on my own to address this situation?

Under Massachusetts law, you have the right to obtain any police report filed regarding this incident. If you are the victim of identity theft, you also have the right to file a police report and receive a copy of it.

Massachusetts law also allows consumers to place a security freeze on their credit reports at no cost to the consumer. A security freeze prohibits a credit reporting agency from releasing any information from a consumer's credit report without written authorization. However, please be aware that placing a security freeze on your credit report may delay, interfere with, or prevent the timely approval of any requests you make for new loans, credit mortgages, employment, housing or other services.

To place a security freeze on your credit report, you will need to contact **each** of the three major consumer reporting agencies by phone, online or via mail at the addresses below:

Equifax Security Freeze
1-800-685-1111
P.O. Box 105788
Atlanta, GA 30348
Equifax.com/personal/credit-report-services

Experian Security Freeze
P.O. Box 9554
Allen, TX 75013
Experian.com/help

Trans Union Security Freeze
Fraud Victim Assistance Department
P.O. Box 2000
Chester, PA
19022-2000
Transunion.com/credit-help

To request a security freeze, you will need to provide the following information:

- Your full name (including middle initial as well as Jr., Sr., II, III, etc.)
- address
- Social Security Number
- Date of birth

If you submit a request for a security freeze via mail, you may be asked to provide the additional information:

- If you have moved in the past five (5) years, provide the addresses where you have lived over the prior five years
- Proof of current address such as a recent utility bill or telephone bill
- A legible photocopy of a government-issued identification card (state driver's license or I.D. card, military identification, etc.)
- If you are a victim of identity theft, include a copy of either the police report, investigative report, or complaint to a law enforcement agency concerning identity theft

The credit reporting agencies have three (3) business days to place a security freeze on your credit report after receiving your request. The credit bureaus must also send written confirmation to you within five (5) business days and provide you with a unique personal identification number (PIN) or password, or both that you can use to authorize the removal or lifting of the security freeze.

To lift the security freeze to allow a specific entity or individual access to your credit report, you must call, go online or send a written request to the credit reporting agencies by mail and include proper identification (name, address, and social security number) **and** the PIN number or password provided to you when you placed the security freeze as well as the identities of those entities or individuals you would like to receive your credit report or the specific period of time you want the credit report available. If the request is made online or by phone, the credit reporting agency must lift a freeze within one hour. If the request is made by mail, the credit reporting agencies have three (3) business days after receiving your request to lift the security freeze for those identified entities or for the specified period of time.

To remove the security freeze, you must call, go online or send a written request by mail to each of the three credit bureaus and include proper identification (name, address, and social security number) **and** the PIN number or password provided to you when you placed the security freeze. If the request is made online or by phone, the credit reporting agency must lift a freeze within one hour. If the request is made by mail, the credit reporting agencies have three (3) business days after receiving your request to lift the security freeze permanently.

What else can I do on my own to address this situation?

We recommend that you consider taking one or more of the following steps to obtain additional information and minimize chances of identity theft.

1. Place a 90-day fraud alert on your credit file

An initial 90-day security alert indicates to anyone requesting your credit file that you suspect you are a victim of fraud. When you or someone else attempts to open a credit account in your name, increase the credit limit on an existing account, or obtain a new card on an existing account, the lender should take steps to verify that you have authorized the request. If the credit

cannot verify that you have authorized this, the request should not be satisfied. You may contact any one of the credit reporting companies below for assistance.

Experian: 1-888-397-3742; www.experian.com

TransUnion: 1-800-680-7289; www.transunion.com

Equifax: 1-800-525-6285; www.equifax.com

2. Order your free annual credit reports

Consider visiting www.annualcreditreport.com or call 877-322-8228 to order your free annual credit reports. Once you receive your credit reports, review them for discrepancies, identify any accounts you did not open, or inquiries from creditors that you did not authorize. Verify all information is correct. If you have questions or notice any incorrect information, contact the credit reporting company.

Equifax	Experian	TransUnion
P.O. Box 740256	P.O. Box 2390	P.O. Box 1000
Atlanta, GA 30374	Allen, TX 75013	Chester, PA 19022
(866) 510-4211	(866) 751-1323	(800) 888-4213
psol@equifax.com	databreachinfo@experian.com	https://tudatabreach.tnwreports.com
www.equifax.com	www.experian.com/	www.transunion.com

3. Manage your personal information

You can take steps that include carrying only essential documents with you, being aware of with whom you share your personal information, and shredding receipts, statements, and other sensitive information.

4. Remove your name from mailing lists of pre-approved offers of credit for approximately six months.

By calling 1-888-567-8688, you can obtain a form to remove your name from pre-approved credit card offers. You will need to share some personal information, such as your name, Social Security Number and date of birth when you submit your request. For more information on opting out of prescreen offers of credit, please refer to:

http://www.ftc.gov/bcp/edu/pubs/consumer/credit/cre17.shtm

5. Use Tools from Credit Providers

Carefully review your credit reports and bank, credit card, and other account statements. Be proactive and create alerts on your credit cards and bank accounts for notice of activity. If you discover unauthorized or suspicious activity on your credit report or by any other means, contact

your creditor or bank immediately and file an identity theft report with your local police and contact a credit reporting company.

6. Report suspected identity fraud

You can file a report of suspected incidents of identity theft with local law enforcement, your state Attorney General, or the Federal Trade Commission.

To obtain additional information about identity theft and ways to protect yourself contact the Federal Trade Commission ("FTC") either by visiting www.ftc.gov, www.consumer.gov/idtheft, or by calling (877) 438-4338. If you suspect or know that you are the victim of identity theft, you can report this to the Fraud Department of the FTC, who will collect all information and make it available to law-enforcement agencies. Contact information for the FTC is: 877-436-4338, TTY 866-653-4261.

Federal Trade Commission
Consumer Response Center
600 Pennsylvania Avenue
NW Washington, DC 20580

In addition to the FTC, you also may contact your state's attorney general's office and the credit reporting agencies above to provide you with information about fraud alerts and security freezes.

What if I want to speak with Rockefeller Archive Center regarding this incident?

While call center representatives should be able to provide thorough assistance and answer most of your questions, you may still feel the need to speak with Rockefeller Archive Center regarding this incident. You may also contact Brigite Requeijo at (914) 366-6381 if you have any questions.

At the Rockefeller Archive Center, we take our responsibility to protect your personal information seriously, and we truly regret any concern this incident may cause you.

Sincerely,

Jack Meyers

Jack Meyers

4861-3866-5989, v. 1

Notice of Data Breach

Dear <<First Name>> <<Last Name>>,

As a current or former patient of Rockefeller Archive Center, we are notifying you of a data incident that may have involved your protected health information and personal information.

What Happened

On November 2, 2021, Rockefeller Archive Center learned it was the victim of a sophisticated cybersecurity attack. We promptly took steps to secure our network and engaged a third-party cybersecurity firm to conduct a forensic investigation into the cause and scope of the attack. The investigation determined that an unauthorized individual had gained access to our network. The individual did not access Rockefeller Archive Center's electronic medical records application; however, the individual deployed malware and accessed or acquired certain documents in our systems that contain patient information.

What Information Was Involved

This information may have included the following: name, address, date of birth, medical information such as office notes and diagnostic reports and, in limited circumstances, a Social Security Number. At this time, we have no indication that any of your information has been used to commit identity theft or fraud.

What We Are Doing

Rockefeller Archive Center endeavors to protect the privacy and security of patient information. We are working diligently to determine how this incident happened and taking appropriate measures to prevent a similar situation in the future.

What You Can Do

As with any data incident, we recommend that you remain vigilant and consider taking steps to avoid identity theft, obtain additional information, and protect your personal information. We have included a list of suggested measures at the end of this letter.

For More Information

We apologize for any concern this incident may cause you. Please call [TFN] or go to https://response.idx.us/customending for assistance or for any additional questions you may have.

Sincerely,
Jack Meyers
Rockefeller Archive Center

(Enclosure)

Recommended Steps to Help Protect Your Information

1. Place a 90-day fraud alert on your credit file. An initial 90-day security alert indicates to anyone requesting your credit file that you suspect you are a victim of fraud. When you or someone else attempts to open a credit account in your name, increase the credit limit on an existing account, or obtain a new card on an existing account, the lender should take steps to verify that you have authorized the request. If the credit cannot verify that you have authorized this, the request should not be satisfied. You may contact one of the credit reporting companies below for assistance.
   Experian: 1-888-397-3742; www.experian.com
   TransUnion: 1-800-680-7289; www.transunion.com
   Equifax: 1-800-525-6285; www.equifax.com

2. Place a security freeze on your credit. Placing a freeze on your credit report will prevent lenders and others from accessing your credit report, which will prevent them from extending credit. With a security freeze in place, you will be required to take special steps when you wish to apply for any type of credit. This process is also accessed through each of the credit reporting companies and there is no charge.
   To place a security freeze on your credit report, you must send a written request to each of the three major consumer reporting agencies by regular, certified or overnight mail at the addresses below or, if available, comply with the consumer reporting agencies' online security freeze request procedures:

Equifax Security Freeze 1-888-298-0045	Experian Security Freeze	Trans Union Security Freeze
P.O. Box 105788	1-888-397-3742	1-888-909-8872
Atlanta, GA 30348	P.O. Box 9554	P.O. Box 160
www.equifax.com	Allen, TX 75013	Woodlyn, PA 19094
	www.experian.com	www.transunion.com

In order to request a security freeze, you may need to provide the following information:

1. Your full name (including middle initial as well as Jr., Sr., II, III, etc.);
2. Social Security Number;
3. Date of birth;
4. If you have moved in the past five (5) years, provide the addresses where you have lived over the prior five years;
5. Proof of current address such as a current utility bill or telephone bill;
6. A legible photocopy of a government issued identification card (state driver's license or ID card, military identification, etc.); and
7. If you are a victim of identity theft, include a copy of either the police report, investigative report, or complaint to a law enforcement agency concerning identity theft.

The credit reporting agencies have three (3) business days after receiving your request to place a security freeze on your credit report. The credit bureaus must also send written confirmation to you within five (5) business days and provide you with a unique personal identification number (PIN) or password, or both that can be used by you to authorize the removal or lifting of the security freeze.

To lift the security freeze in order to allow a specific entity or individual access to your credit report, you must call or send a written request to the credit reporting agencies by mail or, if available, comply with the consumer

reporting agencies' online procedures for lifting a security freeze, and include proper identification (name, address, and social security number) and the PIN number or password provided to you when you placed the security freeze as well as the identities of those entities or individuals you would like to receive your credit report or the specific period of time you want the credit report available. The credit reporting agencies have three (3) business days after receiving your request to lift the security freeze for those identified entities or for the specified period of time.

To remove the security freeze, you must send a written request to each of the three credit bureaus by mail or, if available, comply with the consumer reporting agencies' online procedures for removing a security freeze, and include proper identification (name, address, and social security number) and the PIN number or password provided to you when you placed the security freeze. The credit bureaus have three (3) business days after receiving your request to remove the security freeze.

3. Order your free annual credit reports. Visit www.annualcreditreport.com or call 877-322-8228 to obtain a free annual credit report. Once you receive your credit report, review it for discrepancies, identify accounts you did not open or inquiries from creditors that you did not authorize, and verify all information is correct. If you have questions, or notice any incorrect information, contact the credit reporting company.

Equifax	Experian	TransUnion
P.O. Box 740256	P.O. Box 2390	P.O. Box 1000
Atlanta, GA 30374	Allen, TX 75013	Chester, PA 19022
(866) 510-4211	(866) 751-1323	(800) 888-4213
psol@equifax.com	databreachinfo@experian.com	https://tudatabreach.tnwreports.com/
www.equifax.com	www.experian.com/	www.transunion.com

4. Use tools from credit providers and monitor your statements. Carefully review your credit reports and bank, credit card, and other account statements. Be proactive and create alerts on your credit cards and bank accounts for notice of activity. If you discover unauthorized or suspicious activity on your credit report or by any other means, file an identity theft report with your local police and contact a credit reporting company. We also recommend that you review the statements you receive from your healthcare provider and health insurer. If you see any charges for services that you did not receive, please call the provider or insurer immediately.

5. Report suspected identity theft. You have the right to file a police report if you ever experience identity fraud. Please note that in order to file a crime report or incident report with law enforcement for identity theft, you will likely need to provide some kind of proof that you have been a victim. A police report is often required to dispute fraudulent items. You can report suspected incidents of identity theft to local law enforcement, the Attorney General, or the Federal Trade Commission.

6. Your Rights Under the Fair Credit Reporting Act: The Fair Credit Reporting Act (FCRA) establishes procedures to correct mistakes on your credit record and requires that your record be made available only for certain legitimate business needs. Under the FCRA, both the credit bureau and the organization that provided the information to the credit bureau (the "information provider"), such as a bank or credit card company, are responsible for correcting inaccurate or incomplete information in your report. Your major rights under the FCRA are summarized below.

   - You must be told if information in your file has been used against you.
   - You have the right to know what is in your file.
   - You have the right to ask for a credit score.
   - You have the right to dispute incomplete or inaccurate information.
   - Consumer reporting agencies 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 reports to be provided to employers.

- You may limit "prescreened" offers of credit and insurance you get based on information in your credit report.
- You have a right to place a "security freeze" on your credit report, which will prohibit a consumer reporting agency from releasing information in your credit report without your express authorization.
- You may seek damages from violators.
- Identity theft victims and active duty military personnel have additional rights.

To protect your rights under the law, contact both the credit bureau and the information provider. For additional information, visit www.consumerfinance.gov/learnmore or write to: Consumer Financial Protection Bureau, 1700 G Street NW, Washington, DC 20552.

0. For information on Medical Identity Theft, please see the Federal Trade Commission (FTC) brochure, Medical Identity Theft (consumer.ftc.gov/articles/0171-medical-identity-theft.

1. To contact the FTC, or for additional information on identity theft, please call or contact the FTC at 877-436-4338, TTY 866-653-4261.
   www.ftc.gov/idtheft.
   Federal Trade Commission
   Consumer Response Center
   600 Pennsylvania Avenue
   NW Washington, DC 20580

2. Residents of Maryland: You may obtain information about preventing identity theft from the following source: Office of the Attorney General, 200 St. Paul Place, Baltimore, MD 21202, (410) 576-6491, and http://www.marylandattorneygeneral.gov/Pages/IdentityTheft/default.aspx.

   Residents of New York: You may obtain additional information from the New York State Police, 1220 Washington Avenue, Building 22, Albany, NY 12226-2252 or https://www.troopers.ny.gov/ and the Division of Consumer Protection, One Commerce Plaza, 99 Washington Ave., Suite 640, Albany, NY 12231, Phone: (800) 697-1220 and https://www.dos.ny.gov/consumerprotection/.

   Residents of North Carolina: you may obtain information about preventing identity theft from the following source: Office of the Attorney General, 0001 Mail Service Center, Raleigh, NC 27699-9001, (919) 716-6400, and www.ncdoj.gov/Home/ContactNCDOJ.aspx.

   Residents of Oregon: You may obtain information about preventing identity theft from the following source: Office of the Attorney General, Oregon Department of Justice, 1162 Court Street NE, Salem, OR 97301-4096; (503) 378-4400 and http://www.doj.state.or.us/Pages/Index.aspx.