



ROPES & GRAY LLP  
2099 PENNSYLVANIA AVENUE, NW  
WASHINGTON, DC 20006-6807  
WWW.ROPESGRAY.COM

February 19, 2020

Edward R. McNicholas  
T +1 202 508 4779  
edward.mcnicholas@ropesgray.com

**BY E-MAIL**

Attorney General Gordon MacDonald  
Consumer Protection Bureau  
Office of the Attorney General  
33 Capitol Street  
Concord, NH 03301  
[DOJ-CPB@doj.nh.gov](mailto:DOJ-CPB@doj.nh.gov)

Re: Data Incident

Dear General MacDonald:

We write on behalf of our client, Advocate Aurora Health (“AAH”), to inform you of a recent security incident that may have affected the personal information of 13 New Hampshire residents.

Our investigation is still ongoing. As we understand the incident currently, on or about January 1, 2020, an unauthorized individual used a phishing campaign targeted at AAH to gain access to several AAH employees’ email credentials. For one of these employees who works in payroll, these credentials allowed access to the PeopleSoft system, which houses personal information including social security numbers, home contact and dependent information, and direct deposit banking information for current and former AAH employees.

AAH first became aware of the incident on January 9, 2020, when the attacker succeeded in diverting payroll deposits for some 44 persons and changing the information for an additional 19 persons. Soon thereafter, all affected credentials were changed, and the intruder was locked out of the system. AAH then reset all passwords across the potentially affected systems and has begun to deploy Proofpoint email filtering and Duo multi-factor authentication to further secure its systems.

Subsequent investigation has revealed both that the attacker had access to the entire PeopleSoft system and that logging is not sufficient to rule out further unauthorized access of that system. Accordingly, out of an abundance of caution, AAH is considering all portions of the PeopleSoft system accessible via the compromised credentials to be compromised, resulting in notices being

ROPES & GRAY LLP

Attorney General Gordon MacDonald

- 2 -

February 19, 2020

sent to roughly 176,000 current and former employees, who reside primarily in Wisconsin, Illinois, and Michigan.

We have also notified and are working with federal and Wisconsin state law enforcement. FBI Supervisory Special Agent Amanda Knutsen in Wisconsin is the senior lead. We are cooperating fully with these investigations as our own investigation continues.

We have attached a sample of the notification made to the affected parties. If you have any questions, please reach out to us at +1 (202)-508-4779.

Sincerely,

A handwritten signature in cursive script that reads "Edward R. McNicholas".

Edward R. McNicholas



Return Mail Processing  
PO Box 589  
Claysburg, PA 16625-0589

February 20, 2020



F3433-L07-0000007 P001 T00001 \*\*\*\*\*MIXED AADC 159  
SAMPLE A SAMPLE - L07 AURORA ALL OTHER  
APT 123  
123 ANY ST  
ANYTOWN, US 12345-6789



***RE: Notice of Security Incident  
Please read this entire letter.***

Dear Sample A Sample:

We are writing to share with you some important information regarding a recent incident that may have involved your personal information.

**What Happened?**

At the beginning of January 2020, an individual not authorized by Advocate Aurora Health had temporary access to certain employee credentials through an email phishing campaign. Our early findings indicate that there was unauthorized access to a human resource system that houses personal information for current and former employees. Once Advocate Aurora became aware of the incident on Jan. 9, affected credentials were changed, and the intruder was locked out of the system.

**What Information Was Involved?**

Our early findings indicate that some of our team members and their information may have been impacted. The investigation is ongoing. At present, we understand the following. For team members who currently work or formerly worked at a Wisconsin location, the information includes the team member’s Social Security number, the bank account used for direct deposit, birth date and home address.

**What Are We Doing?**

In addition to changing the credentials for affected Advocate Aurora accounts, we have taken further steps to increase security and protect your personal information. We immediately launched an investigation and notified federal and state law enforcement.

**What Can You Do?**

As always, we encourage you to regularly review your financial accounts and report any suspicious or unrecognized activity immediately. The enclosed “Important Identity Theft Information” provides further information about what you can do. As recommended by federal regulatory agencies, you should remember to be vigilant for the next 12 to 24 months and report any suspected incidents of fraud to the relevant financial institution.

0000007



To help protect your identity, we are offering a complimentary one-year membership of Experian's® IdentityWorks<sup>SM</sup>. To activate your membership and start monitoring your personal information please follow the steps below:

- Ensure that you **enroll by: May 31, 2020** (Your code will not work after this date.)
- **Visit** the Experian IdentityWorks website to enroll: <https://www.experianidworks.com/3bcredit>
- Provide your **activation code: ABCDEFGHI**

For more information on identity theft prevention and IdentityWorks, including instructions on how to activate your complimentary one-year membership, please see the attached "**Additional Details Regarding Your Experian Identityworks Membership.**"

If you have questions about the product, need assistance with identity restoration or would like an alternative to enrolling in Experian IdentityWorks online, please contact Experian's customer care team at 1.855.359.3624 by **May 31, 2020**. Be prepared to provide engagement number **ENGAGE#** as proof of eligibility for the identity restoration services by Experian.

#### **Other Important Information.**

We take all data security matters seriously and apologize for any inconvenience. Should you have any further questions please visit [www.aah.org/cybersecurity](http://www.aah.org/cybersecurity) or call 1.855.359.3624.

Sincerely,



Mike Lappin  
Chief Administrative Officer

## ADDITIONAL DETAILS REGARDING YOUR EXPERIAN IDENTITYWORKS MEMBERSHIP

A credit card is **not** required for enrollment in Experian IdentityWorks.

You can contact Experian **immediately** regarding any fraud issues, and have access to the following features once you enroll in Experian IdentityWorks:

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

If you believe there was fraudulent use of your information and would like to discuss how you may be able to resolve those issues, please reach out to an Experian agent at 1.855.359.3624. If, after discussing your situation with an agent, it is determined that Identity Restoration support is needed, then an Experian Identity Restoration agent is available to work with you to investigate and resolve each incident of fraud that occurred (including, as appropriate, helping you with contacting credit grantors to dispute charges and close accounts; assisting you in placing a freeze on your credit file with the three major credit bureaus; and assisting you with contacting government agencies to help restore your identity to its proper condition).

Please note that this Identity Restoration support is available to you for one year from the date of this letter and does not require any action on your part at this time. The Terms and Conditions for this offer are located at [www.ExperianIDWorks.com/restoration](http://www.ExperianIDWorks.com/restoration). You will also find self-help tips and information about identity protection at this site.

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

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



**IMPORTANT IDENTITY THEFT INFORMATION:  
ADDITIONAL STEPS YOU CAN TAKE TO PROTECT YOUR IDENTITY**

Review Your Accounts and Credit Reports

Regularly review statements from your accounts and periodically obtain your credit report from one or more of the national credit reporting companies. You may obtain a free copy of your credit report online at [www.annualcreditreport.com](http://www.annualcreditreport.com) by calling toll free 1.877.322.8228, or by mailing an Annual Credit Report Request Form (available at [www.annualcreditreport.com](http://www.annualcreditreport.com)) to: Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA, 30348-5281. You may also purchase a copy of your credit report by contacting one or more of the three national credit reporting agencies listed below:

- **Equifax**, P.O. Box 740241, Atlanta, Georgia 30374-0241. 1.800.685.1111. [www.equifax.com](http://www.equifax.com)
- **Experian**, P.O. Box 9532, Allen, TX 75013. 1.888.397.3742. [www.experian.com](http://www.experian.com)
- **TransUnion**, 2 Baldwin Place, P.O. Box 1000, Chester, PA 19016. 1.800.916.8800. [www.transunion.com](http://www.transunion.com)

Consider Placing a Fraud Alert

You may wish to consider contacting the fraud department of the three major credit bureaus to request that a “fraud alert” be placed on your file. A fraud alert notifies potential lenders to verify your identification before extending credit in your name.

Equifax:	Report Fraud:	1.800.766.0008
Experian:	Report Fraud:	1.888.397.3742
TransUnion:	Report Fraud:	1.800.680.7289

Security Freeze for Credit Reporting Agencies

You may wish to request a security freeze on your credit reports. 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. It is free to place, lift or remove a security freeze.

You must separately place a security freeze on your credit report at each credit bureau. To do so, you must contact the credit bureaus by phone, mail, or secure electronic means:

- **Equifax**: P.O. Box 105788, Atlanta, GA 30348, 1.800.349.9960, [www.Equifax.com](http://www.Equifax.com)
- **Experian**: P.O. Box 9554, Allen, TX 75013, 1.888.397.3742, [www.Experian.com](http://www.Experian.com)
- **TransUnion**: P.O. Box 2000, Chester, PA 19106, 1.888.909.8872, [www.TransUnion.com](http://www.TransUnion.com)

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

- Your full name (including middle initial, Jr., Sr., Roman numerals, etc.),
- Social Security number
- Date of birth
- Address(es) where you have lived over the prior five years
- Proof of current address such as a current utility bill
- A photocopy of a government-issued ID card
- 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

If you request a freeze online or by phone, the agency must place the freeze within one business day. The credit bureaus have three business days after receiving a request by mail to place a security freeze on your credit report, and they must also send confirmation to you within five 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 freeze to allow a specific entity or individual access to your credit report, you must contact the credit reporting agencies and include (1) proper identification; (2) the PIN number or password provided to you when you placed the security freeze; and (3) 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.

You have rights under the federal Fair Credit Reporting Act (FCRA). These include, among others, the right to know what is in your file; to dispute incomplete or inaccurate information; and to have consumer reporting agencies correct or delete inaccurate, incomplete, or unverifiable information. For more information about the FCRA, please visit [www.consumer.ftc.gov/articles/pdf-0096-fair-credit-reporting-act.pdf](http://www.consumer.ftc.gov/articles/pdf-0096-fair-credit-reporting-act.pdf) or [www.ftc.gov](http://www.ftc.gov).

### Suggestions if You Are a Victim of Identity Theft

- File a police report. Get a copy of the report to submit to your creditors and others that may require proof of a crime.
- Contact the U.S. Federal Trade Commission (FTC). The FTC provides useful information to identity theft victims and maintains a database of identity theft cases for use by law enforcement agencies. File a report with the FTC by calling the FTC's Identity Theft Hotline: 1-877-IDTHEFT (438-4338); online at <http://www.ftc.gov/idtheft>; or by mail at Identity Theft Clearinghouse, Federal Trade Commission, 600 Pennsylvania Ave., N.W., Washington, D.C. 20580. Also request a copy of the publication, "Take Charge: Fighting Back Against Identity Theft" from [https://www.consumer.ftc.gov/articles/pdf-0009\\_identitytheft\\_a\\_recovery\\_plan.pdf](https://www.consumer.ftc.gov/articles/pdf-0009_identitytheft_a_recovery_plan.pdf)
- Keep a record of your contacts. Start a file with copies of your credit reports, the police reports, any correspondence, and copies of disputed bills. It is helpful to log conversations with creditors, law enforcement officials, and other relevant parties.

### Take Steps to Avoid Identity Theft

Further information can be obtained from the FTC about steps to take to avoid identity theft at: <http://www.ftc.gov/idtheft>; calling 1-877-IDTHEFT (438-4338); or write to Consumer Response Center, Federal Trade Commission, 600 Pennsylvania Ave., N.W., Washington, D.C. 20580.

### State Specific Information

**Iowa residents** may contact law enforcement or the Iowa Attorney General's Office to report suspected incidents of identity theft. This office can be reached by visiting the website at [www.iowaattorneygeneral.gov](http://www.iowaattorneygeneral.gov), calling (515) 281-5164 or requesting more information from the Office of the Attorney General, Hoover State Office Building, 1305 E. Walnut Street, Des Moines, IA 50319.

**Maryland residents** can learn more about preventing identity theft from the Maryland Office of the Attorney General, by visiting their web site at <http://www.marylandattorneygeneral.gov/Pages/IdentityTheft/default.aspx>, calling the Identity Theft Unit at 1.410.567.6491, or requesting more information at the Identity Theft Unit, 200 St. Paul Place, 16<sup>th</sup> Floor, Baltimore, MD 21202.

**New Mexico residents** are reminded that you have the right to obtain a police report and request a security freeze as described above and you have rights under the Fair Credit Reporting Act as described above.

**North Carolina residents** can learn more about preventing identity theft from the North Carolina Office of the Attorney General, by visiting their web site at <https://ncdoj.gov/protecting-consumers/identity-theft/calling>

000007



1.919.716.6400 or requesting more information from the North Carolina Attorney General's Office, 9001 Mail Service Center Raleigh, NC 27699-9001.

**Oregon residents** may obtain information about preventing identity theft from the Oregon Attorney General's Office. This office can be reached by visiting the website at [www.doj.state.or.us](http://www.doj.state.or.us), calling (503) 378-4400 or requesting more information from the Oregon Department of Justice, 1162 Court Street NE, Salem, OR 97301-4096.

**Rhode Island residents** are reminded that you have the right to obtain a police report and request a security freeze as described above. The consumer reporting agencies may require that you provide certain personal information (such as your name, Social Security Number, date of birth and address) and proper identification (such as a copy of a government-issued ID card and a bill or statement) prior to honoring your request. Residents can learn more by contacting the Rhode Island Office of the Attorney General by phone at 1.410.274.4400 or by mail at 150 South Main Street, Providence, Rhode Island 02903.

**Vermont residents** may learn helpful information about fighting identity theft, placing a security freeze, and obtaining a free copy of your credit report on the Vermont Attorney General's website at <https://ago.vermont.gov/>.