

April 17, 2020

F4787-L01-0000001 P001 T00001 \*\*\*\*\*MIXED AADC 159



SAMPLE A SAMPLE - L01 PHI ONLY

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 and/or health information.

**What Happened?**

On or about Jan. 1, 2020, an unauthorized individual(s) used an email phishing campaign to gain access to the email credentials of several Advocate Aurora Health employees at Aurora Medical Center - Bay Area. Advocate Aurora learned of this intrusion on or about Jan. 9, 2020 and promptly initiated an internal investigation. Through this investigation, Advocate Aurora confirmed that the intruder(s) did not access Advocate Aurora's or Aurora Medical Center - Bay Area's electronic health record systems. Unfortunately, the investigation revealed that the intruder(s) may have accessed without authorization the emails of certain employees, during a period from approximately Jan. 1, 2020 to Jan. 9, 2020.

While Advocate Aurora cannot confirm that the intruder(s) used the email credentials to access the emails of these employees, Advocate Aurora's review of these email accounts determined that the personal and/or health information of certain Aurora Medical Center - Bay Area patients may have been included in accessible email messages. As such, we are providing this notice to you.

**What Information Was Involved?**

The intruder(s) may have had access to your personal and/or health information, which may have included: your first and/or last name; maiden name; marital status; date of birth; street address, email address and phone number(s); date(s) of admission, discharge or treatment; social security number; medical record number; health insurance account number(s); medical device number(s); driver's license number; passport number; bank or financial account number(s); or full face photographs.

**What Are We Doing?**

Upon discovering the incident, Advocate Aurora launched an internal investigation and notified federal and state law enforcement. We are cooperating fully with law enforcement and continuing our own internal investigation, which includes a forensic investigation performed by external information technology consultants.

0000001



Advocate Aurora has also taken steps to enhance information security at Aurora Medical Center - Bay Area, including changing the credentials for affected Aurora Medical Center - Bay Area employee accounts in January 2020 and resetting the passwords for all Aurora Medical Center - Bay Area workforce members across potentially affected Advocate Aurora systems in January and early February 2020. Aurora Medical Center - Bay Area has also made other technical system enhancements, including an email filtering software to help Advocate Aurora workforce members better identify potential phishing emails.

The privacy and security of patient information is a priority of Advocate Aurora and Aurora Medical Center - Bay Area. We will continue to monitor our information security systems and make improvements and enhancements where appropriate.

### **What Can You Do?**

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.

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: 7.12.20** (Your code will not work after this date.)
- **Visit** the Experian IdentityWorks website to enroll: [www.website.com](http://www.website.com)
- Provide your **activation code: ABCDEFGHI**

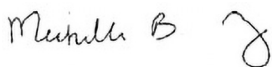
For more information on identity theft prevention and IdentityWorks, including instructions on how to activate your complimentary one-year membership, please see the attached "**Additional Details Regarding Your Experian Identityworks Membership.**"

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 (866) 242-1807 by **7.12.20**. Be prepared to provide engagement number **ENGAGE#** as proof of eligibility for the identity restoration services by Experian.

### **Other Important Information.**

We are very sorry that this incident occurred involving your personal and/or health information. We take all data security matters seriously and apologize for any inconvenience. Should you have any further questions please visit [www.aah.org/patient-cybersecurity](http://www.aah.org/patient-cybersecurity) or call (866) 242-1807.

Sincerely,



Michelle Bergholz Frazier, JD, CHC  
Chief Compliance 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 (866) 242-1807. 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> 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.

**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/>.

April 17, 2020

F4787-L02-0000002 P001 T00001 \*\*\*\*\*MIXED AADC 159



SAMPLE A SAMPLE - L02 PHI\_PRIOR PII

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 additional important information regarding a recent incident that may have involved your personal and/or health information.

**What Happened?**

As you may recall, on or about Jan. 1, 2020, an unauthorized individual(s) used an email phishing campaign to gain access to the email credentials of several Advocate Aurora Health employees at Aurora Medical Center - Bay Area. Advocate Aurora learned of this intrusion on or about Jan. 9, 2020 and promptly initiated an internal investigation. Through this investigation, Advocate Aurora confirmed that the intruder(s) did not access Advocate Aurora's or Aurora Medical Center - Bay Area's electronic health record systems. Unfortunately, the investigation revealed that the intruder(s) may have accessed without authorization the emails of certain employees, during a period from approximately Jan. 1, 2020 to Jan. 9, 2020.

While Advocate Aurora cannot confirm that the intruder(s) used the email credentials to access the emails of these employees, Advocate Aurora's review of these email accounts determined that the personal and/or health information of certain Aurora Medical Center - Bay Area patients may have been included in accessible email messages. As such, we are providing this additional notice to you because your personal and/or health information was included within the accessible email accounts as a patient.

**What Information Was Involved?**

The intruder(s) may have had access to your personal and/or health information, which may have included: your first and/or last name; maiden name; marital status; date of birth; street address, email address and phone number(s); date(s) of admission, discharge or treatment; social security number; medical record number; health insurance account number(s); medical device number(s); driver's license number; passport number; bank or financial account number(s); or full face photographs.

0000002



## What Are We Doing?

Upon discovering the incident, Advocate Aurora launched an internal investigation and notified federal and state law enforcement. We are cooperating fully with law enforcement and continuing our own internal investigation, which includes a forensic investigation performed by external information technology consultants.

Advocate Aurora has also taken steps to enhance information security at Aurora Medical Center - Bay Area, including changing the credentials for affected Aurora Medical Center - Bay Area employee accounts in January 2020 and resetting the passwords for all Aurora Medical Center - Bay Area workforce members across potentially affected Advocate Aurora systems in January and early February 2020. Aurora Medical Center - Bay Area has also made other technical system enhancements, including an email filtering software to help Advocate Aurora workforce members better identify potential phishing emails.

The privacy and security of patient information is a priority of Advocate Aurora and Aurora Medical Center - Bay Area. We will continue to monitor our information security systems and make improvements and enhancements where appropriate.

## What Can You Do?

We encourage you to continue 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.

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: 7.12.20** (Your code will not work after this date.)
- **Visit** the Experian IdentityWorks website to enroll: [www.website.com](http://www.website.com)
- Provide your **activation code: ABCDEFGHI**

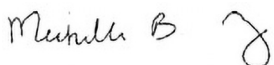
For more information on identity theft prevention and IdentityWorks, including instructions on how to activate your complimentary one-year membership, please see the attached "**Additional Details Regarding Your Experian Identityworks Membership.**"

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 (866) 242-1807 by **7.12.20**. Be prepared to provide engagement number **ENGAGE#** as proof of eligibility for the identity restoration services by Experian.

## Other Important Information.

We are very sorry that this incident occurred involving your personal and/or health information. We take all data security matters seriously and apologize for any inconvenience. Should you have any further questions please visit [www.aah.org/patient-cybersecurity](http://www.aah.org/patient-cybersecurity) or call (866) 242-1807.

Sincerely,



Michelle Bergholz Frazier, JD, CHC  
Chief Compliance 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 (866) 242-1807. 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> 1.919.716.6400 or requesting more information from the North Carolina Attorney General's Office, 9001 Mail Service Center Raleigh, NC 27699-9001.

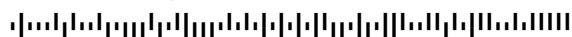
**Oregon residents** may obtain information about preventing identity theft from the Oregon Attorney General's Office. This office can be reached by visiting the website at [www.doj.state.or.us](http://www.doj.state.or.us), calling (503) 378-4400 or requesting more information from the Oregon Department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

**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/>.

April 17, 2020



F4787-L03-0000003 P001 T00001 \*\*\*\*\*MIXED AADC 159  
SAMPLE A SAMPLE - L03 PHI ONLY\_MINORS  
APT 123  
123 ANY ST  
ANYTOWN, US 12345-6789



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

To the Parent or Guardian of Sample A Sample:

We are writing to share with you some important information regarding a recent incident that may have involved your minor's personal and/or health information.

**What Happened?**

On or about Jan. 1, 2020, an unauthorized individual(s) used an email phishing campaign to gain access to the email credentials of several Advocate Aurora Health employees at Aurora Medical Center - Bay Area. Advocate Aurora learned of this intrusion on or about Jan. 9, 2020 and promptly initiated an internal investigation. Through this investigation, Advocate Aurora confirmed that the intruder(s) did not access Advocate Aurora's or Aurora Medical Center - Bay Area's electronic health record systems. Unfortunately, the investigation revealed that the intruder(s) may have accessed without authorization the emails of certain employees, during a period from approximately Jan. 1, 2020 to Jan. 9, 2020.

While Advocate Aurora cannot confirm that the intruder(s) used the email credentials to access the emails of these employees, Advocate Aurora's review of these email accounts determined that the personal and/or health information of certain Aurora Medical Center - Bay Area patients may have been included in accessible email messages. As such, we are providing this notice to you.

**What Information Was Involved?**

The intruder(s) may have had access to your minor's personal and/or health information, which may have included: first and/or last name; maiden name; marital status; date of birth; street address, email address and phone number(s); date(s) of admission, discharge or treatment; social security number; medical record number; health insurance account number(s); medical device number(s); driver's license number; passport number; bank or financial account number(s); or full face photographs.

**What Are We Doing?**

Upon discovering the incident, Advocate Aurora launched an internal investigation and notified federal and state law enforcement. We are cooperating fully with law enforcement and continuing our own internal investigation, which includes a forensic investigation performed by external information technology consultants.

0000003



Advocate Aurora has also taken steps to enhance information security at Aurora Medical Center - Bay Area, including changing the credentials for affected Aurora Medical Center - Bay Area employee accounts in January 2020 and resetting the passwords for all Aurora Medical Center - Bay Area workforce members across potentially affected Advocate Aurora systems in January and early February 2020. Aurora Medical Center - Bay Area has also made other technical system enhancements, including an email filtering software to help Advocate Aurora workforce members better identify potential phishing emails.

The privacy and security of patient information is a priority of Advocate Aurora and Aurora Medical Center - Bay Area. We will continue to monitor our information security systems and make improvements and enhancements where appropriate.

### **What Can You Do?**

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.

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

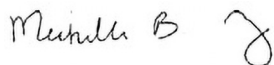
- Ensure that you **enroll by: 7.12.20** (Your code will not work after this date.)
- **Visit** the Experian IdentityWorks website to enroll: [www.website.com](http://www.website.com)
- Provide your **activation code: ABCDEFGHI**
- Provide your minor's information when prompted

If you have questions about the product, need assistance with identity restoration for your minor or would like an alternative to enrolling in Experian IdentityWorks online, please contact Experian's customer care team at (866) 242-1807 by **7.12.20**. Be prepared to provide engagement number **ENGAGE#** as proof of eligibility for the identity restoration services by Experian.

### **Other Important Information.**

We are very sorry that this incident occurred involving your minor's personal and/or health information. We take all data security matters seriously and apologize for any inconvenience. Should you have any further questions please visit [www.aah.org/patient-cybersecurity](http://www.aah.org/patient-cybersecurity) or call (866) 242-1807.

Sincerely,



Michelle Bergholz Frazier, JD, CHC  
Chief Compliance 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 for your minor:

- **Social Security Number Trace:** Monitoring to determine whether enrolled minors in your household have an Experian credit report. Alerts of all names, aliases and addresses that become associated with your minor's Social Security Number (SSN) on the Experian credit report.
- **Internet Surveillance:** Technology searches the web, chat rooms & bulletin boards 24/7 to identify trading or selling of your personal information on the Dark Web.
- **Identity Restoration:** Identity Restoration specialists are immediately available to help you address credit and non-credit related fraud.
- **Experian IdentityWorks ExtendCARE™:** Receive the same high-level of Identity Restoration support even after the 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 minor's information and would like to discuss how you may be able to resolve those issues, please reach out to an Experian agent at (866) 242-1807. 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 your minor 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> 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.

**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/>.