



21779

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

July 16, 2021

G6139-L01-0000001 T00001 P001 *****SCH 5-DIGIT 32808



SAMPLE A. SAMPLE - L01 ADULT
APT ABC
123 ANY ST
ANYTOWN, ST 12345-6789



RE: Notice of Data Breach
Please read this entire letter.

Dear Sample A. Sample:

We are writing to share some important information with you regarding a recent data security incident experienced by a company called Elekta, Inc. ("Elekta") that provides technology services to us. Due to the nature of the services that Elekta provides, the data security incident that they experienced may have affected your personal health information. In this notice, you will find information about the incident, the response, and steps you may take to further protect your personal health information.

What Happened?

Advocate Aurora Health ("Advocate Aurora") uses the services of Elekta to coordinate delivery of radiation services and therapies to patients in most of our Illinois hospitals. In early April 2021, Elekta notified Advocate Aurora that it had experienced a data security incident related to one of its information cloud storage systems that hosted and stored Advocate Aurora patient information.

Upon learning of this incident, Elekta temporarily suspended access to this cloud system and engaged a forensic investigator to investigate the nature and scope of the incident. While Elekta was able to re-launch Advocate Aurora's use of the system in mid-April, Elekta also suffered a further security incident. This, along with the ongoing forensic investigation of the initial data security incident, caused Elekta to terminate use of this cloud system in late April and migrate Advocate Aurora information to its newer information technology platform. Advocate Aurora undertook coordinated efforts to ensure minimal disruption to the delivery of patient care.

On or about May 17, 2021, through continuing engagement of its forensic investigator, Elekta notified Advocate Aurora that the information security system intrusions Elekta experienced in April 2021 resulted in potential access to, and theft of, Advocate Aurora patient health information. Although Elekta could not confirm specifically what information may have been accessed or stolen, it was unable to rule out the possibility that your personal health information may have been compromised.

Advocate Aurora is providing this notice to you out of an abundance of caution as Elekta's records indicate that your personal health information was stored on its system. At this time, there is no indication that your personal health information has been disclosed publicly or used for any fraudulent purpose as a result of this incident.

0000001



What Information Was Involved?

The following information may have been stored on Elekta's systems: your first and/or last name; social security number; street address; date of birth; height; weight; driver's license number; medical diagnosis; medical treatment details; appointment confirmations; and other information that Advocate Aurora may have about you. No financial account, credit card, or debit card information was involved in this incident.

What Are We Doing?

Both Advocate Aurora and Elekta take this incident and the security of patient information very seriously. Upon learning of this incident, Elekta launched an in-depth investigation of the incident by engaging a third-party forensic investigator, and Elekta has taken steps to prevent any further access to information from its systems. Elekta also promptly notified Advocate Aurora of the incident. Immediately after we were notified of the incident, we began working with Elekta to better understand the nature and scope of the incident and coordinate our efforts to continue safely treating patients while keeping all information secure.

As an added precaution, Elekta is also offering complimentary access to identity monitoring, fraud consultation, and identity theft restoration services. If you wish to receive these services, activation instructions are below.

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® IdentityWorksSM. To activate your membership and start monitoring your personal information please follow the steps below:

- Ensure that you **enroll by**: September 10, 2021 (Your code will not work after this date.)
- Visit the Experian IdentityWorks website to enroll: <https://www.experianidworks.com/credit>
- 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.**"

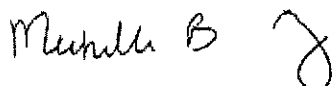
If you have questions about the product, need assistance with identity restoration or would like an alternative to enrolling in Experian IdentityWorks online, please contact Experian's customer care team at (833) 796-8636 by September 10, 2021. Be prepared to provide engagement number **B015669** as proof of eligibility for the identity restoration services by Experian.

Other Important Information.

Both Advocate Aurora and Elekta apologize for the inconvenience that this incident may cause. We take all data security matters seriously and are taking steps to minimize the chances of a similar occurrence happening again.

We understand that you may have questions about this incident that are not addressed in this letter. If you have additional questions, please call our dedicated assistance line at (833) 796-8636, Monday through Friday from 9 a.m. to 11 p.m. Eastern, and Saturday and Sunday from 11 a.m. to 8 p.m. Eastern.

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 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 (833) 796-8636. 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. 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 by calling toll free 1.877.322.8228, or by mailing an Annual Credit Report Request Form (available at www.annualcreditreport.com) to: Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA, 30348-5281. You may also purchase a copy of your credit report by contacting one or more of the three national credit reporting agencies listed below:

- **Equifax**, P.O. Box 740241, Atlanta, Georgia 30374-0241. 1.800.685.1111. www.equifax.com
- **Experian**, P.O. Box 9532, Allen, TX 75013. 1.888.397.3742. www.experian.com
- **TransUnion**, 2 Baldwin Place, P.O. Box 1000, Chester, PA 19016. 1.800.916.8800. 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:	1.800.525.6285
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
- **Experian:** P.O. Box 9554, Allen, TX 75013, 1.888.397.3742, www.Experian.com
- **TransUnion:** P.O. Box 2000, Chester, PA 19106, 1.888.909.8872, 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 or 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>
- 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

District of Columbia residents may obtain information from the FTC and the Office of the Attorney General for the District of Columbia about steps to take to avoid identity theft. You can contact the D.C. Attorney General at: 441 4th Street, NW, Washington, DC 20001, 202-727-3400, www.oag.dc.gov.

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, 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, 16th Floor, Baltimore, MD 21202.



Massachusetts residents have a right to request from us a copy of any police report filed in connection with 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. As noted above, you also have the right to place a security freeze on your credit report at no charge.

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.

New York residents may also contact the following state agencies for information regarding security breach response and identity theft prevention and protection information:

New York Attorney General's Office
Bureau of Internet and Technology
(212) 416-8433
<https://ag.ny.gov/internet/resource-center>

NYS Department of State's Division of Consumer
Protection
(800) 697-1220
<https://www.dos.ny.gov/consumerprotection>

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, 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/>.



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

July 16, 2021

G6139-L02-0000002 T00001 P001 *****SCH 5-DIGIT 32808



SAMPLE A. SAMPLE - L02 CT ADULT
APT ABC
123 ANY ST
ANYTOWN, ST 12345-6789



RE: Notice of Data Breach
Please read this entire letter.

To the Parent or Guardian of Sample A. Sample:

We are writing to share some important information with you regarding a recent data security incident experienced by a company called Elekta, Inc. ("Elekta") that provides technology services to us. Due to the nature of the services that Elekta provides, the data security incident that they experienced may have affected your minor's personal health information. In this notice, you will find information about the incident, the response, and steps you may take to further protect your minor's personal health information.

What Happened?

Advocate Aurora Health ("Advocate Aurora") uses the services of Elekta to coordinate delivery of radiation services and therapies to patients in most of our Illinois hospitals. In early April 2021, Elekta notified Advocate Aurora that it had experienced a data security incident related to one of its information cloud storage systems that hosted and stored Advocate Aurora patient information.

Upon learning of this incident, Elekta temporarily suspended access to this cloud system and engaged a forensic investigator to investigate the nature and scope of the incident. While Elekta was able to re-launch Advocate Aurora's use of the system in mid-April, Elekta also suffered a further security incident. This, along with the ongoing forensic investigation of the initial data security incident, caused Elekta to terminate use of this cloud system in late April and migrate Advocate Aurora information to its newer information technology platform. Advocate Aurora undertook coordinated efforts to ensure minimal disruption to the delivery of patient care.

On or about May 17, 2021, through continuing engagement of its forensic investigator, Elekta notified Advocate Aurora that the information security system intrusions Elekta experienced in April 2021 resulted in potential access to, and theft of, Advocate Aurora patient health information. Although Elekta could not confirm specifically what information may have been accessed or stolen, it was unable to rule out the possibility that your minor's personal health information may have been compromised.

Advocate Aurora is providing this notice to you out of an abundance of caution as Elekta's records indicate that your minor's personal health information was stored on its system. At this time, there is no indication that your minor's personal health information has been disclosed publicly or used for any fraudulent purpose as a result of this incident.

0000002



What Information Was Involved?

The following information may have been stored on Elekta's systems: your minor's first and/or last name; social security number; street address; date of birth; height; weight; driver's license number; medical diagnosis; medical treatment details; appointment confirmations; and other information that Advocate Aurora may have about your minor. No financial account, credit card, or debit card information was involved in this incident.

What Are We Doing?

Both Advocate Aurora and Elekta take this incident and the security of patient information very seriously. Upon learning of this incident, Elekta launched an in-depth investigation of the incident by engaging a third-party forensic investigator, and Elekta has taken steps to prevent any further access to information from its systems. Elekta also promptly notified Advocate Aurora of the incident. Immediately after we were notified of the incident, we began working with Elekta to better understand the nature and scope of the incident and coordinate our efforts to continue safely treating patients while keeping all information secure.

As an added precaution, Elekta is also offering complimentary access to identity monitoring, fraud consultation, and identity theft restoration services. If your minor wishes to receive these services, activation instructions are below.

What Can You Do?

We encourage you to regularly review your minor's 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® IdentityWorksSM. 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**: September 10, 2021 (Your code will not work after this date.)
- **Visit** the Experian IdentityWorks website to enroll: <https://www.experianidworks.com/minorplus>
- Provide your **activation code**: ABCDEFGHI
- Provide your minor's information when prompted

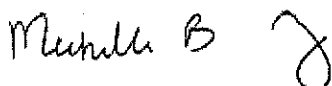
If you have questions about the product, need assistance with identity restoration for your minor or would like an alternative to enrolling in Experian IdentityWorks online, please contact Experian's customer care team at (833) 796-8636 by September 10, 2021. Be prepared to provide engagement number **B015978** as proof of eligibility for the identity restoration services by Experian.

Other Important Information.

Both Advocate Aurora and Elekta apologize for the inconvenience that this incident may cause. We take all data security matters seriously and are taking steps to minimize the chances of a similar occurrence happening again.

We understand that you may have questions about this incident that are not addressed in this letter. If you have additional questions, please call our dedicated assistance line at (833) 796-8636, Monday through Friday from 9 a.m. to 11 p.m. Eastern, and Saturday and Sunday from 11 a.m. to 8 p.m. Eastern.

Sincerely,



Michelle Bergholz Frazier, JD, CHC
Chief Compliance Officer

ADDITIONAL DETAILS REGARDING THE 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 (833) 796-8636. 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. You will also find self-help tips and information about identity protection at this site.

* 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 by calling toll free 1.877.322.8228, or by mailing an Annual Credit Report Request Form (available at www.annualcreditreport.com) to: Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA, 30348-5281. You may also purchase a copy of your credit report by contacting one or more of the three national credit reporting agencies listed below:

- **Equifax**, P.O. Box 740241, Atlanta, Georgia 30374-0241. 1.800.685.1111. www.equifax.com
- **Experian**, P.O. Box 9532, Allen, TX 75013. 1.888.397.3742. www.experian.com
- **TransUnion**, 2 Baldwin Place, P.O. Box 1000, Chester, PA 19016. 1.800.916.8800. 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:	1.800.525.6285
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
- **Experian**: P.O. Box 9554, Allen, TX 75013, 1.888.397.3742, www.Experian.com
- **TransUnion**: P.O. Box 2000, Chester, PA 19106, 1.888.909.8872, 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 or 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 identify 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>
- 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

District of Columbia residents may obtain information from the FTC and the Office of the Attorney General for the District of Columbia about steps to take to avoid identity theft. You can contact the D.C. Attorney General at: 441 4th Street, NW, Washington, DC 20001, 202-727-3400, www.oag.dc.gov.

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, 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, 16th Floor, Baltimore, MD 21202.



Massachusetts residents have a right to request from us a copy of any police report filed in connection with 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. As noted above, you also have the right to place a security freeze on your credit report at no charge.

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.

New York residents may also contact the following state agencies for information regarding security breach response and identity theft prevention and protection information:

New York Attorney General's Office
Bureau of Internet and Technology
(212) 416-8433
<https://ag.ny.gov/internet/resource-center>

NYS Department of State's Division of Consumer
Protection
(800) 697-1220
<https://www.dos.ny.gov/consumerprotection>

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, 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/>.

July 16, 2021

[RECIPIENT NAME]
[RECIPIENT ADDRESS]
[CITY, STATE ZIP]

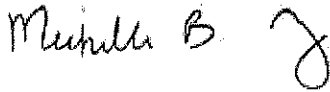
Re: Updates to Notice of Data Breach

Dear [RECIPIENT NAME]:

You previously received a letter from us concerning a recent data security incident experienced by a company called Elekta, Inc. (“Elekta”) that provides technology services to us. Due to a technical issue, your letter incorrectly states that you are eligible for only one year of complimentary access to identity monitoring, fraud consultation, and identity theft restoration services. We are writing to assure you that you are being offered a complimentary two-year membership to Experian’s® IdentityWorksSM. Please follow the steps listed and provide the activation code in your original letter to activate your two-year membership.

If you have additional questions, please call our dedicated assistance line at (833) 796-8636, Monday through Friday from 9 a.m. to 11 p.m. Eastern, and Saturday and Sunday from 11 a.m. to 8 p.m. Eastern.

Sincerely,



Michelle Bergholz Frazier, JD, CHC
Chief Compliance Officer