

June 27, 2024

By Email

Office of the Attorney General
Consumer Protection Division
200 St. Paul Place
Baltimore, MD 21202
consumer@oag.state.md.us

Re: Ann & Robert H. Lurie Children's
Hospital of Chicago Cybersecurity Attack

To Whom It May Concern:

Ann & Robert H. Lurie Children's Hospital of Chicago ("Lurie Children's") writes to provide formal notice of a sophisticated cybersecurity attack Lurie Children's experienced earlier this year. This notice is made consistent with Lurie Children's obligations under Maryland Commercial Code § 14-3501.

Lurie Children's has determined that cybercriminals accessed Lurie Children's systems between January 26 and 31, 2024 through credential compromise and ransomware. Lurie Children's has determined that cybercriminals accessed Lurie Children's between January 26 and 31, 2024. On January 31, 2024, to protect its systems and its ability to continue operations, Lurie Children's took certain electronic systems offline, including email, phones, the electronic health record system (Epic), and Epic's patient portal (MyChart). Lurie Children's activated its standard incident response procedures, including the Hospital Incident Command Structure (HICS). Additionally, Lurie Children's retained leading cybersecurity experts and legal counsel to work with its internal teams. Lurie Children's has worked closely with federal law enforcement as well. No threat actor activity has been identified in Lurie Children's' environment since January 31, 2024.

Our investigation included a thorough and methodical review and analysis of impacted data on our systems. Lurie Children's has determined through its ongoing investigation that Personal Information (as that term is defined in Md. Comm. Code § 14-3501(1)) relating to approximately 234 Maryland residents, including patients and current and former team members, was impacted. Lurie Children's is notifying individuals whose information was impacted in the cybersecurity attack, including through mailing notification letters and media and substitute notice. Enclosed are the two templates for the notification letters Lurie Children's is mailing to Maryland residents. Additionally, Lurie Children's is offering complimentary access to Experian IdentityWorksSM for 24 months to Maryland residents whose information was impacted in the cybersecurity matter.

We take the privacy and security of our patients' and team members' sensitive data very seriously. As explained above, Lurie Children's took prompt steps to secure our systems, and we engaged third-party experts to assist in the investigation. Since the cybersecurity attack, we have implemented additional cybersecurity safeguards and we are working closely with our internal and external experts to further enhance the security of our systems.

The information submitted herein is proprietary and confidential and should be afforded confidential treatment. If you have any questions, please contact our legal counsel Scott Lashway of Mintz, Levin, Cohn, Ferris, Glovsky and Popeo, P.C. at (617) 348-1833 or slashway@mintz.com.

Sincerely,

Max Siegel, JD, CHC
Chief Compliance and Integrity Officer |
Privacy Officer

Enclosures

June 27, 2024



L5025-L09-0022908 T00089 P003 *****5-DIGIT 60618



Re: Notice of Data Breach

Dear [REDACTED]:

Ann & Robert H. Lurie Children's Hospital of Chicago ("Lurie Children's") has been investigating the nature and scope of a sophisticated cybersecurity attack that occurred earlier this year. Lurie Children's is writing to update you about the cybersecurity attack and to inform you that your information was impacted. We are providing information about the measures Lurie Children's has taken in response to this matter, and steps you can take to help protect against possible misuse of information.

What Happened

Through Lurie Children's' ongoing investigation, Lurie Children's has determined that cybercriminals accessed Lurie Children's systems between January 26 and 31, 2024. On January 31, 2024, to protect our systems and our ability to continue operations, Lurie Children's took certain electronic systems offline, including our email, phones, and electronic health record system (Epic), and Epic's patient portal (MyChart). Lurie Children's activated our standard incident response procedures, including the Hospital Incident Command Structure. Additionally, Lurie Children's retained leading cybersecurity experts and legal counsel to work with our internal teams. Lurie Children's has worked closely with law enforcement as well. No threat actor activity has been identified in Lurie Children's' environment since January 31, 2024.

Our investigation included a thorough and methodical review and analysis of impacted data on our systems. Through our ongoing investigation, Lurie Children's has determined that certain individuals' personally identifiable and/or protected health information was impacted.

You have been identified as an individual whose information was impacted in this cybersecurity attack. We are notifying you to provide information and steps you can take to help protect your information.

B124406



What Information Was Involved

At this time, we believe the information impacted may have included [REDACTED]
[REDACTED].

What We Are Doing

We take the privacy and security of your data very seriously. As explained above, Lurie Children's took steps to secure our systems, and we engaged third-party experts to assist in the investigation. Since the cybersecurity attack, we have implemented additional cybersecurity safeguards, and we are working closely with our internal and external experts to further enhance the security of our systems.

Additionally, to help protect your identity, we are offering complimentary access to Experian IdentityWorksSM for 24 months.

If you believe there was fraudulent use of your information as a result of this incident and would like to discuss how you may be able to resolve those issues, please reach out to an Experian agent. 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 from the date of the incident (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 Identity Restoration is available to you for 24 months 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 <https://www.ExperianIDWorks.com/restoration>.

While identity restoration assistance is immediately available to you, we also encourage you to activate the fraud detection tools available through Experian IdentityWorks as a complimentary 24-month membership. This product provides you with superior identity detection and resolution of identity theft. To start monitoring your personal information, please follow the steps below:

- Ensure that you enroll by October 5, 2024 (Your code will not work after this date.)
- Visit the Experian IdentityWorks website to enroll: <https://www.experianidworks.com/credit>
- Provide your activation code: [REDACTED]

If you have questions about the product, need assistance with Identity Restoration that arose as a result of this incident, or would like an alternative to enrolling in Experian IdentityWorks online, please contact Experian's customer care team at 888-401-0575 by October 5, 2024. Be prepared to provide engagement number B124406 as proof of eligibility for the Identity Restoration services by Experian.

ADDITIONAL DETAILS REGARDING YOUR 24-MONTH 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 file 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.
- **\$1 Million Identity Theft Insurance†:** Provides coverage for certain costs and unauthorized electronic fund transfers.

What You Can Do

It is always a good practice to remain vigilant and to carefully review your online accounts, financial statements, and Explanations of Benefits from your health insurers for any unauthorized activity. Contact the company that maintains the account immediately if you detect any suspicious transactions or other activity you do not recognize. You should also report suspected incidents of identity theft to local law enforcement or your state's attorney general.

For More Information

If you have further questions or concerns, or would like an alternative to enrolling online, please call 888-401-0575 toll-free, 8 am to 8 pm, Central Time, Monday through Friday (excluding major U.S. holidays). Be prepared to provide your engagement number B124406.

At Lurie Children's, we take the privacy of our patients' and team members' sensitive information very seriously. We deeply regret that this cybersecurity attack occurred.

Sincerely,

Max Siegel, JD, CHC
Chief Compliance and Integrity Officer | Privacy Officer
Ann & Robert H. Lurie Children's Hospital of Chicago

* 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.



ADDITIONAL ACTIONS TO HELP REDUCE YOUR CHANCES OF IDENTITY THEFT

➤ PLACE A 90-DAY FRAUD ALERT ON YOUR CREDIT FILE

A Fraud Alert is a consumer statement added to your credit report that alerts creditors of possible fraudulent activity within your report as well as requests that they contact you prior to establishing any accounts in your name. An initial 90-day security alert indicates to anyone requesting your credit file that you suspect you are a victim of fraud. Once the fraud alert is added to your credit report, when you or someone else attempts to open a credit account in your name, increase the credit limit on an existing account, or obtain a new card on an existing account, the lender should take steps to verify that you have authorized the request. If the creditor cannot verify this, the request should not be satisfied. You may contact one of the credit reporting companies below for assistance.

Equifax
PO Box 105069
Atlanta, GA 30348
1-888-378-4329
www.equifax.com

Experian
PO Box 2002
Allen, TX 75013
1-888-397-3742
www.experian.com

TransUnion
PO Box 2000
Chester, PA 19016
1-800-916-8800
www.transunion.com

➤ PLACE AN EXTENDED FRAUD ALERT ON YOUR CREDIT FILE

You may also want to consider contacting the credit reporting companies and asking them to place an extended fraud alert. If you are a victim of identity theft and have created an Identity Theft Report, you can place an extended fraud alert on your credit file. It stays in effect for 7 years. When you place an extended alert, you can get 2 free credit reports within 12 months from each of the 3 nationwide credit reporting companies, and the credit reporting companies must take your name off marketing lists for prescreened credit offers for 5 years, unless you ask them to put your name back on the list.

➤ SECURITY FREEZE ON YOUR CREDIT FILE

If you are very concerned about becoming a victim of fraud or identity theft, a security freeze might be right for you. Placing a freeze on your credit report will prevent lenders and others from accessing your credit report entirely, which will prevent them from extending credit. With a Security Freeze in place, you will be required to take special steps when you wish to apply for any type of credit. This process is completed through each of the credit reporting companies. To obtain a security freeze from all credit reporting agencies, impacted individuals must contact each credit reporting agency separately and complete their respective security freeze request process. Under federal law, you cannot be charged to place or lift a credit freeze from a credit report. To obtain a security freeze each credit reporting agency will require you to provide certain information to prove your identity, which may include your Full Name, Current and Prior Addresses, Social Security Number, Date of Birth, and/or Identification Card. Special state-by-state rules may apply regarding the availability of security freezes for minors.

- For information regarding Experian's security freeze process, see:
<https://www.experian.com/freeze/center.html>
- For information regarding TransUnion's security freeze process, see:
<https://www.transunion.com/credit-freeze/place-credit-freeze>
- For information regarding Equifax's security freeze process, see:
<https://www.equifax.com/personal/credit-report-services/credit-freeze>

➤ **ORDER YOUR FREE ANNUAL CREDIT REPORTS**

Visit <https://www.annualcreditreport.com> or call 877-322-8228.

Once you receive your credit reports, review them for discrepancies. Identify any accounts you did not open or inquiries from creditors that you did not authorize. Verify all information is correct. If you have questions or notice incorrect information, contact the credit reporting company.

➤ **MANAGE YOUR PERSONAL INFORMATION**

Take steps such as: carrying only essential documents with you; being aware of whom you are sharing your personal information with and shredding receipts, statements, and other sensitive information.

We recommend that you regularly review the explanation of benefits statement that you receive from your insurer. If you see any service that you believe you did not receive, please contact your insurer at the number on the statement. If you do not receive regular explanation of benefits statements, contact your provider and request them to send such statements following the provision of services in your name or number.

You may want to order copies of your credit reports and check for any medical bills that you do not recognize. If you find anything suspicious, call the credit reporting agency at the phone number on the report. Keep a copy of this notice for your records in case of future problems with your medical records. You may also want to request a copy of your medical records from your provider, to serve as a baseline.

➤ **USE TOOLS FROM CREDIT PROVIDERS**

Carefully review your credit reports and bank, credit card and other account statements. Be proactive and create alerts on credit cards and bank accounts to notify you of activity. If you discover unauthorized or suspicious activity on your credit report or by any other means, file an identity theft report with your local police and contact a credit reporting company.

➤ **BE ON THE LOOKOUT FOR PHISHING SCHEMES**

We recommend that you be on the lookout for suspicious emails. Specifically, be on the lookout for phishing schemes, which are attempts by criminals to steal personal information, including credit card numbers and social security numbers, over email. These attempts are often made by manipulating an email to make it look as if it came from a legitimate source, but which is actually sent by a fraudulent impersonator.

Pay particular attention to anyone asking you to click on a link or attachment, especially if the email requests sensitive information, and pay close attention to the email address (look for misspellings in the email address). It is also important that you check the recipient's email address when replying to emails to ensure it is legitimate.

➤ **POLICE REPORT**

You may also have the right to file or obtain a police report.

➤ **SUMMARY OF YOUR RIGHTS UNDER THE FAIR CREDIT REPORTING ACT:**

The Federal Trade Commission ("FTC") has created the following summary of consumer rights under the Fair Credit Reporting Act, available at https://files.consumerfinance.gov/f/201504_cfpb_summary_your-rights-under-fcra.pdf. Notably, the FTC states that: "The federal Fair Credit Reporting Act (FCRA) promotes the accuracy, fairness, and privacy of information in the files of consumer reporting agencies. There are many types of consumer reporting agencies, including credit bureaus and specialty agencies (such as agencies that sell information about check writing histories, medical records, and rental history records). Here is a



summary of your major rights under the FCRA. For more information, including information about additional rights, go to www.ftc.gov/credit or write to: Consumer Response Center, Room 130-A, Federal Trade Commission, 600 Pennsylvania Ave. N.W., Washington, D.C. 20580.” As outlined in the FTC’s summary, these rights include, but are not limited to the following:

- “You must be told if information in your file has been used against you.”
- “You have the right to know what is in your file.”
- “You have the right to ask for a credit score.”
- “You have the right to dispute incomplete or inaccurate information.”
- “Consumer reporting agencies must correct or delete inaccurate, incomplete, or unverifiable information.”
- “Consumer reporting agencies may not report outdated negative information.”
- “Access to your file is limited.”
- “You must give your consent for reports to be provided to employers.”
- “You may limit ‘prescreened’ offers of credit and insurance you get based on information in your credit report.”
- “You may seek damages from violators.”
- “Identity theft victims and active duty military personnel have additional rights.”

➤ **OBTAIN MORE INFORMATION ABOUT IDENTITY THEFT AND WAYS TO PROTECT YOURSELF**

We recommend you remain vigilant with respect to reviewing your account statements and credit reports, and promptly report any suspicious activity or suspected identity theft to us and to the proper law enforcement authorities, including local law enforcement, your state’s attorney general and/or the Federal Trade Commission (“FTC”). You may contact the FTC or your state’s regulatory authority to obtain additional information about avoiding identity theft.

Federal Trade Commission, 600 Pennsylvania Avenue, NW, Washington, DC 20580, 1-877-IDTHEFT (438-4338), www.ftc.gov/idtheft

For residents of the District of Columbia: You may also obtain information about preventing and avoiding identity theft from the District of Columbia Attorney General:

District of Columbia Office of the Attorney General, Consumer Protection
441 4th Street, NW, Washington, DC 20001, 1-202-442-9828,
<https://oag.dc.gov/consumer-protection>

For residents of Iowa: You may also obtain information about preventing and avoiding identity theft from the Iowa Office of the Attorney General:

Iowa Office of the Attorney General, Consumer Protection Division
1305 E. Walnut Street, Des Moines, Iowa 50319-0106, 1-515-281-5926,
<https://www.iowaattorneygeneral.gov/for-consumers/security-breach-notifications/>

For residents of Maryland: You may also obtain information about preventing and avoiding identity theft from the Maryland Office of the Attorney General:

Maryland Office of the Attorney General, Consumer Protection Division
200 St. Paul Place, Baltimore, MD 21202, 1-888-743-0023,
<https://www.marylandattorneygeneral.gov/Pages/CPD>

For residents of Massachusetts: You also have the right to obtain a police report.

For residents of New Mexico: You have rights under the federal Fair Credit Reporting Act (“FCRA”). For more information, see above section “SUMMARY OF YOUR RIGHTS

UNDER THE FAIR CREDIT REPORTING ACT” or visit
https://files.consumerfinance.gov/f/201504_cfpb_summary_your-rights-under-fcra.pdf.

For residents of New York: You may also obtain information about preventing and avoiding identity theft from the New York Attorney General:

New York Office of the Attorney General, Consumer Frauds and Protection Bureau
The Capitol, Albany, NY 12224,
<https://ag.ny.gov/resources/individuals/consumer-issues/technology>

For residents of North Carolina: You may also obtain information about preventing and avoiding identity theft from the North Carolina Attorney General’s Office:

North Carolina Attorney General’s Office, Consumer Protection Division
9001 Mail Service Center, Raleigh, NC 27699-9001, 1-877-5-NO-SCAM,
www.ncdoj.gov

For residents of Oregon: You may also obtain information about preventing and avoiding identity theft from the Oregon Department of Justice:

Oregon Department of Justice, Consumer Protection
1162 Court Street NE, Salem, OR 97301-4096
1-877-877-9392, <https://www.doj.state.or.us/consumer-protection/id-theft-data-breaches/data-breaches/>

For residents of Rhode Island: You also have the right to obtain a police report. You may also obtain information about preventing and avoiding identity theft from the Rhode Island Office of the Attorney General:

Rhode Island Office of the Attorney General, Consumer Protection Unit
150 South Main Street, Providence, RI 02903, 1-401-274-4400,
<http://www.riag.ri.gov/ConsumerProtection/About.php>

For residents of West Virginia: You also have the right to obtain a security freeze. You may obtain a security freeze on your credit report to protect your privacy and ensure that credit is not granted in your name without your knowledge. You may also obtain information about preventing and avoiding identity theft from the West Virginia Attorney General’s Office:

West Virginia Attorney General’s Office, Consumer Protection Division
P.O. Box 1789, Charleston, WV 25326, Toll-Free: 1-800-368-8808, Phone:
304-558-8986, <http://www.ago.wv.gov/consumerprotection/pages/identity-theft-prevention.aspx>





**Ann & Robert H. Lurie
Children's Hospital of Chicago**

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

June 27, 2024

L5025-L10-0009732 T00038 P001 *****SCH 5-DIGIT 60015

TO THE PARENT OR GUARDIAN OF:



Re: Notice of Data Breach

Dear Parent or Guardian of [REDACTED]:

Ann & Robert H. Lurie Children's Hospital of Chicago ("Lurie Children's") has been investigating the nature and scope of a sophisticated cybersecurity attack that occurred earlier this year. Lurie Children's is writing to update you about the cybersecurity attack and to inform you that your child's or minor dependent's information was impacted. We are providing information about the measures Lurie Children's has taken in response to this matter, and steps you can take to help protect against possible misuse of information.

What Happened

Through Lurie Children's' ongoing investigation, Lurie Children's has determined that cybercriminals accessed Lurie Children's systems between January 26 and 31, 2024. On January 31, 2024, to protect our systems and our ability to continue operations, Lurie Children's took certain electronic systems offline, including our email, phones, and electronic health record system (Epic), and Epic's patient portal (MyChart). Lurie Children's activated our standard incident response procedures, including the Hospital Incident Command Structure. Additionally, Lurie Children's retained leading cybersecurity experts and legal counsel to work with our internal teams. Lurie Children's has worked closely with law enforcement as well. No threat actor activity has been identified in Lurie Children's' environment since January 31, 2024.

Our investigation included a thorough and methodical review and analysis of impacted data from our systems. Through our ongoing investigation, Lurie Children's has determined that certain individuals' personally identifiable and/or protected health information was impacted.

Your child or minor dependent has been identified as an individual whose information was impacted in this cybersecurity attack. We are notifying you to provide information and steps you can take to help protect your child's or minor dependent's information.

0009732



B124407

L5025-L10

What Information Was Involved

At this time, we believe the information impacted may have included [REDACTED]

What We Are Doing

We take the privacy and security of your child's or minor dependent's data very seriously. As explained above, Lurie Children's took steps to secure our systems, and we engaged third-party experts to assist in the investigation. Since the cybersecurity attack, we have implemented additional cybersecurity safeguards, and we are working closely with our internal and external experts to further enhance the security of our systems.

Additionally, to help protect your child's or minor dependent's identity, we are offering complimentary access to Experian IdentityWorksSM for 24 months.

If you believe there was fraudulent use of your child's or minor dependent's information as a result of this incident and would like to discuss how you may be able to resolve those issues, please reach out to an Experian agent. 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 from the date of the incident (including, as appropriate, helping you with contacting credit grantors to dispute charges and close accounts; assisting you in placing a freeze on your child's or minor dependent's credit file with the three major credit bureaus; and assisting you with contacting government agencies to help restore your child's or minor dependent's identity to its proper condition).

Please note that Identity Restoration is available to your child or minor dependent for 24 months 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 <https://www.ExperianIDWorks.com/restoration>.

While identity restoration assistance is immediately available to your child or minor dependent, we also encourage you to activate the fraud detection tools available through Experian IdentityWorks as a complimentary 24-month membership. This product provides your child or minor dependent with superior identity detection and resolution of identity theft. To start monitoring your child's or minor dependent's personal information, please follow the steps below:

- Ensure that you enroll by October 5, 2024 (Your code will not work after this date.)
- Visit the Experian IdentityWorks website to enroll: <https://www.experianidworks.com/minorplus>
- Provide your activation code: [REDACTED]
- Provide your child's or minor dependent's information when prompted

If you have questions about the product, need assistance with Identity Restoration that arose as a result of this incident or would like an alternative to enrolling in Experian IdentityWorks online, please contact Experian's customer care team at 888-401-0575 by October 5, 2024. Be prepared to provide engagement number B124407 as proof of eligibility for the Identity Restoration services by Experian.

ADDITIONAL DETAILS REGARDING YOUR MINOR'S 24-MONTH 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 your child or minor dependent in Experian IdentityWorks:

- **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 child's or minor dependent'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 child's or minor dependent's 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™:** You receive the same high-level of Identity Restoration support even after your child's or minor dependent's Experian IdentityWorks membership has expired.
- **\$1 Million Identity Theft Insurance*:** Provides coverage for certain costs and unauthorized electronic fund transfers.

What You Can Do

It is always a good practice to remain vigilant and to carefully review your and your child's or minor dependent's online accounts, financial statements, and Explanations of Benefits from health insurers for any unauthorized activity. Contact the company that maintains the account immediately if you detect any suspicious transactions or other activity you do not recognize. You should also report suspected incidents of identity theft to local law enforcement or your state's attorney general.

For More Information

If you have further questions or concerns, or would like an alternative to enrolling online, please call 888-401-0575 toll-free, 8 am to 8 pm, Central Time, Monday through Friday (excluding major U.S. holidays). Be prepared to provide your engagement number B124407.

At Lurie Children's, we take the privacy of your child's or minor dependent's sensitive information very seriously. We deeply regret that this cybersecurity attack occurred.

Sincerely,

Max Siegel, JD, CHC
Chief Compliance and Integrity Officer | Privacy Officer
Ann & Robert H. Lurie Children's Hospital of Chicago

* 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.



ADDITIONAL ACTIONS TO HELP REDUCE YOUR CHANCES OF IDENTITY THEFT

➤ PLACE A 90-DAY FRAUD ALERT ON YOUR CREDIT FILE

A Fraud Alert is a consumer statement added to your credit report that alerts creditors of possible fraudulent activity within your report as well as requests that they contact you prior to establishing any accounts in your name. An initial 90-day security alert indicates to anyone requesting your credit file that you suspect you are a victim of fraud. Once the fraud alert is added to your credit report, when you or someone else attempts to open a credit account in your name, increase the credit limit on an existing account, or obtain a new card on an existing account, the lender should take steps to verify that you have authorized the request. If the creditor cannot verify this, the request should not be satisfied. You may contact one of the credit reporting companies below for assistance.

Equifax
PO Box 105069
Atlanta, GA 30348
1-888-378-4329
www.equifax.com

Experian
PO Box 2002
Allen, TX 75013
1-888-397-3742
www.experian.com

TransUnion
PO Box 2000
Chester, PA 19016
1-800-916-8800
www.transunion.com

➤ PLACE AN EXTENDED FRAUD ALERT ON YOUR CREDIT FILE

You may also want to consider contacting the credit reporting companies and asking them to place an extended fraud alert. If you are a victim of identity theft and have created an Identity Theft Report, you can place an extended fraud alert on your credit file. It stays in effect for 7 years. When you place an extended alert, you can get 2 free credit reports within 12 months from each of the 3 nationwide credit reporting companies, and the credit reporting companies must take your name off marketing lists for prescreened credit offers for 5 years, unless you ask them to put your name back on the list.

➤ SECURITY FREEZE ON YOUR CHILD'S OR MINOR DEPENDENT'S CREDIT FILE

If you are very concerned about your child or minor dependent becoming a victim of fraud or identity theft, a security freeze might be right for you. A security freeze prohibits a credit reporting agency from releasing any information from a consumer's credit report without written authorization.

Minors, sixteen years or older, have the right to place a security freeze on a credit report, which will prohibit a consumer reporting agency from releasing information in the credit report without express authorization. A parent or guardian also has the right to place a security freeze on a minor's credit report if the child is under the age of sixteen. If the nationwide credit reporting agencies do not have a credit file on the minor, they will create one so they can freeze it. This record cannot be used for credit purposes. It is there to make sure the minor's record is frozen and protected against potential identify theft and fraud. Pursuant to federal law, you cannot be charged to place or lift a credit freeze from a credit report. Should you wish to place a security freeze on a credit file or proactively place a freeze on your child's or minor dependent's credit report, please contact the major consumer reporting agencies listed below.

To request information about the existence of a credit file in your child's or minor dependent's name, search for your child's or minor dependent's Social Security number, place a security freeze on your child's or minor dependent's credit file, place a fraud alert on your child's or minor dependent's credit report (if it exists), or request a copy of your child's or minor dependent's credit report, you may be required to provide the following information:

- A copy of your driver's license or another government issued identification card, such as a state ID card, etc.;
- Proof of address, such as a copy of a bank statement, utility bill, insurance statement, etc.;

- A copy of your child's or minor dependent's birth certificate;
- A copy of your child's or minor dependent's Social Security card;
- Your child's or minor dependent's full name, including middle initial and generation, such as JR, SR, II, III, etc.;
- Your child's or minor dependent's date of birth; and
- Your child's or minor dependent's addresses for the past two years.

To place a security freeze on your minor's credit report, you must send a written request to each of the three major consumer reporting agencies: Equifax; Experian; and TransUnion by regular, certified or overnight mail at the addresses below:

Equifax Security Freeze
P.O. Box 105788
Atlanta, GA 30348

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

**TransUnion Security Freeze
Fraud Victim Assistance
Department**
P.O. Box 160
Woodlyn, PA 19094

For information regarding
Equifax's security freeze
process, see
<https://www.equifax.com/personal/credit-report-services/credit-freeze>

For information regarding
Experian's security freeze
process, see:
<https://www.experian.com/freeze/center.html>

For information regarding
TransUnion's security freeze
process, see:
<https://www.transunion.com/credit-freeze/place-credit-freeze>

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

To lift the security freeze in order to allow a specific entity or individual access to your minor's credit report, you must call or send a written request to the credit reporting agencies by mail and include proper identification (name, address, and social security number) and the PIN number or password provided to you when you placed the security freeze as well as the identities of those entities or individuals you would like to receive the credit report or the specific period of time you want the credit report available. The credit reporting agencies have three (3) business days after receiving your request to lift the security freeze for those identified entities or for the specified period of time.

To remove the security freeze, you must send a written request to each of the three credit bureaus by mail and include proper identification (name, address, and social security number) and the PIN number or password provided to you when you placed the security freeze. The credit bureaus have three (3) business days after receiving your request to remove the security freeze

➤ **ORDER YOUR FREE ANNUAL CREDIT REPORTS**

Visit <https://www.annualcreditreport.com> or call 877-322-8228.

Once you receive your credit reports, review them for discrepancies. Identify any accounts you did not open or inquiries from creditors that you did not authorize. Verify all information is correct. If you have questions or notice incorrect information, contact the credit reporting company.

➤ **MANAGE YOUR PERSONAL INFORMATION**



Take steps such as: carrying only essential documents with you; being aware of whom you are sharing your personal information with and shredding receipts, statements, and other sensitive information.

We recommend that you regularly review the explanation of benefits statement that you receive from your insurer. If you see any service that you believe you did not receive, please contact your insurer at the number on the statement. If you do not receive regular explanation of benefits statements, contact your provider and request them to send such statements following the provision of services in your name or number.

You may want to order copies of your credit reports and check for any medical bills that you do not recognize. If you find anything suspicious, call the credit reporting agency at the phone number on the report. Keep a copy of this notice for your records in case of future problems with your medical records. You may also want to request a copy of your medical records from your provider, to serve as a baseline.

➤ **USE TOOLS FROM CREDIT PROVIDERS**

Carefully review your credit reports and bank, credit card and other account statements. Be proactive and create alerts on credit cards and bank accounts to notify you of activity. If you discover unauthorized or suspicious activity on your credit report or by any other means, file an identity theft report with your local police and contact a credit reporting company.

➤ **BE ON THE LOOKOUT FOR PHISHING SCHEMES**

We recommend that you be on the lookout for suspicious emails. Specifically, be on the lookout for phishing schemes, which are attempts by criminals to steal personal information, including credit card numbers and social security numbers, over email. These attempts are often made by manipulating an email to make it look as if it came from a legitimate source, but which is actually sent by a fraudulent impersonator.

Pay particular attention to anyone asking you to click on a link or attachment, especially if the email requests sensitive information, and pay close attention to the email address (look for misspellings in the email address). It is also important that you check the recipient's email address when replying to emails to ensure it is legitimate.

➤ **POLICE REPORT**

You may also have the right to file or obtain a police report.

➤ **SUMMARY OF YOUR RIGHTS UNDER THE FAIR CREDIT REPORTING ACT:**

The Federal Trade Commission ("FTC") has created the following summary of consumer rights under the Fair Credit Reporting Act, available at https://files.consumerfinance.gov/f/201504_cfpb_summary_your-rights-under-fcra.pdf. Notably, the FTC states that: "The federal Fair Credit Reporting Act (FCRA) promotes the accuracy, fairness, and privacy of information in the files of consumer reporting agencies. There are many types of consumer reporting agencies, including credit bureaus and specialty agencies (such as agencies that sell information about check writing histories, medical records, and rental history records). Here is a summary of your major rights under the FCRA. For more information, including information about additional rights, go to www.ftc.gov/credit or write to: Consumer Response Center, Room 130-A, Federal Trade Commission, 600 Pennsylvania Ave. N.W., Washington, D.C. 20580." As outlined in the FTC's summary, these rights include, but are not limited to the following:

- "You must be told if information in your file has been used against you."
- "You have the right to know what is in your file."
- "You have the right to ask for a credit score."

- “You have the right to dispute incomplete or inaccurate information.”
- “Consumer reporting agencies must correct or delete inaccurate, incomplete, or unverifiable information.”
- “Consumer reporting agencies may not report outdated negative information.”
- “Access to your file is limited.”
- “You must give your consent for reports to be provided to employers.”
- “You may limit ‘prescreened’ offers of credit and insurance you get based on information in your credit report.”
- “You may seek damages from violators.”
- “Identity theft victims and active-duty military personnel have additional rights.”

➤ **OBTAIN MORE INFORMATION ABOUT IDENTITY THEFT AND WAYS TO PROTECT YOURSELF**

We recommend you remain vigilant with respect to reviewing your account statements and credit reports, and promptly report any suspicious activity or suspected identity theft to us and to the proper law enforcement authorities, including local law enforcement, your state’s attorney general and/or the Federal Trade Commission (“FTC”). You may contact the FTC or your state’s regulatory authority to obtain additional information about avoiding identity theft.

Federal Trade Commission, 600 Pennsylvania Avenue, NW, Washington, DC 20580, 1-877-IDTHEFT (438-4338), www.ftc.gov/idtheft

For residents of the District of Columbia: You may also obtain information about preventing and avoiding identity theft from the District of Columbia Attorney General:

District of Columbia Office of the Attorney General, Consumer Protection
441 4th Street, NW, Washington, DC 20001, 1-202-442-9828,
<https://oag.dc.gov/consumer-protection>

For residents of Iowa: You may also obtain information about preventing and avoiding identity theft from the Iowa Office of the Attorney General:

Iowa Office of the Attorney General, Consumer Protection Division
1305 E. Walnut Street, Des Moines, Iowa 50319-0106, 1-515-281-5926,
<https://www.iowaattorneygeneral.gov/for-consumers/security-breach-notifications/>

For residents of Maryland: You may also obtain information about preventing and avoiding identity theft from the Maryland Office of the Attorney General:

Maryland Office of the Attorney General, Consumer Protection Division
200 St. Paul Place, Baltimore, MD 21202, 1-888-743-0023,
<https://www.marylandattorneygeneral.gov/Pages/CPD>

For residents of Massachusetts: You also have the right to obtain a police report.

For residents of New Mexico: You have rights under the federal Fair Credit Reporting Act (“FCRA”). For more information, see above section “SUMMARY OF YOUR RIGHTS UNDER THE FAIR CREDIT REPORTING ACT” or visit https://files.consumerfinance.gov/f/201504_cfpb_summary_your-rights-under-fcra.pdf.

For residents of New York: You may also obtain information about preventing and avoiding identity theft from the New York Attorney General:

New York Office of the Attorney General, Consumer Frauds and Protection Bureau
The Capitol, Albany, NY 12224,



<https://ag.ny.gov/resources/individuals/consumer-issues/technology>

For residents of North Carolina: You may also obtain information about preventing and avoiding identity theft from the North Carolina Attorney General's Office:

North Carolina Attorney General's Office, Consumer Protection Division
9001 Mail Service Center, Raleigh, NC 27699-9001, 1-877-5-NO-SCAM,
www.ncdoj.gov

For residents of Oregon: You may also obtain information about preventing and avoiding identity theft from the Oregon Department of Justice:

Oregon Department of Justice, Consumer Protection
1162 Court Street NE, Salem, OR 97301-4096
1-877-877-9392, <https://www.doj.state.or.us/consumer-protection/id-theft-data-breaches/data-breaches/>

For residents of Rhode Island: You also have the right to obtain a police report. You may also obtain information about preventing and avoiding identity theft from the Rhode Island Office of the Attorney General:

Rhode Island Office of the Attorney General, Consumer Protection Unit
150 South Main Street, Providence, RI 02903, 1-401-274-4400,
<http://www.riag.ri.gov/ConsumerProtection/About.php>

For residents of West Virginia: You also have the right to obtain a security freeze. You may obtain a security freeze on your credit report to protect your privacy and ensure that credit is not granted in your name without your knowledge. You may also obtain information about preventing and avoiding identity theft from the West Virginia Attorney General's Office:

West Virginia Attorney General's Office, Consumer Protection Division
P.O. Box 1789, Charleston, WV 25326, Toll-Free: 1-800-368-8808, Phone:
304-558-8986, <http://www.ago.wv.gov/consumerprotection/pages/identity-theft-prevention.aspx>