MULLEN COUGHLIN LLC
ATTORNEYS AT LAW

M. Alexandra Belton
Office: (267) 930-4773
Fax: (267) 930-4771
Email: abelton@mullen.law

426 W. Lancaster Avenue, Suite 200
Devon, PA 19333

May 19, 2022

VIA U.S. MAIL

Consumer Protection Bureau
Office of the New Hampshire Attorney General
33 Capitol Street
Concord, NH 03301

Re: Notice of Data Event

Dear Sir or Madam:

We represent East Tennessee Children's Hospital ("ETCH") located at 2018 W Clinch Ave, Knoxville, TN 37916, and write to notify your office of an incident that may affect the security of certain personal information relating to approximately one (1) New Hampshire resident. This notice will be supplemented with any new significant facts learned subsequent to its submission. By providing this notice, ETCH does not waive any rights or defenses regarding the applicability of New Hampshire law, the applicability of the New Hampshire data event notification statute, or personal jurisdiction.

Nature of the Data Event

On March 13, 2022, ETCH identified unusual activity on its network. ETCH promptly began taking steps to secure its systems and commenced a comprehensive investigation into the incident. Through the investigation, on March 18, 2022, ETCH determined that certain documents stored within its environment may have been copied from or viewed on the system by an unauthorized person(s) between March 11, 2022 and March 14, 2022. ETCH then undertook a comprehensive review of the affected data to determine what records were present and to whom the information related. On April 19, 2022, the investigation identified certain patient records present in the affected data. The investigation determined that the affected personal information as defined by N.H. Rev. Stat. § 359-C:19 related to the New Hampshire resident includes: name and Social Security number.

While its investigation was ongoing, on April 7, 2022, before it had determined what patient records may have been viewed or copied on its network, ETCH took steps to report this incident via posting of notice on its website and making notice to the media in relevant jurisdictions. ETCH is now providing written notice to those patients who have been identified through the data review for whom it has address information.

Notice to New Hampshire Resident

On or about May 19, 2022, ETCH will begin providing written notice of this incident to affected individuals. Written notice is being provided in substantially the same form as the letter attached here as ***Exhibit A***. As noted above, ETCH also previously posted notice of this incident to the homepage of its website and provided notice to the media in relevant jurisdictions. These notices were provided in substantially the same form as the communications attached here as ***Exhibits B*** and ***C***, respectively.

Other Steps Taken and To Be Taken

The confidentiality, privacy, and security of information within its care are among ETCH's highest priorities. ETCH moved quickly to investigate and respond to the incident, assess the security of its systems, and identify potentially affected individuals. Further, ETCH notified federal law enforcement regarding the event. ETCH is also working to implement additional safeguards and review and enhance its existing policies and procedures.

ETCH is providing access to credit monitoring services for one (1) year to individuals whose personal information was potentially affected by this incident, at no cost to these individuals. Additionally, ETCH is providing impacted individuals with guidance on how to better protect against identity theft and fraud, including providing individuals with information on how to place a fraud alert and security freeze on one's credit file, the contact details for the national consumer reporting agencies, information on how to obtain a free credit report, a reminder to remain vigilant for incidents of fraud and identity theft by reviewing account statements and monitoring free credit reports, and encouragement to contact the Federal Trade Commission, their state Attorney General, and law enforcement to report attempted or actual identity theft and fraud. ETCH is providing written notice of this incident to relevant state regulators, as necessary, and to the three major credit reporting agencies, Equifax, Experian, and TransUnion. ETCH is also notifying the U.S. Department of Health and Human Services ("HHS").

Contact Information

Should you have any questions regarding this notification or other aspects of the data security event, please contact us at (267) 930-4773.

Very truly yours,

M. Alexandra Belton of
MULLEN COUGHLIN LLC

MABB/jym
Enclosure

EXHIBIT A

East Tennessee Children's Hospital
PO Box 4129
Everett WA 98204

ENDORSE
NAME
ADDRESS1
ADDRESS2
CSZ
COUNTRY
BREAK
SEQ
CODE 2D
Ver 1A

To Enroll, Please Call:
1-833-749-1685
Or Visit:
https://response.idx.us/etch
Enrollment Code: <<XXXXXXXX>>

May 19, 2022

NOTICE OF [SECURITY INCIDENT] / [DATA BREACH]

Dear <<First Name>> <<Last Name>>:

East Tennessee Children's Hospital ("ETCH") is writing to make you aware of a recent incident that may affect the privacy of some of your information. We take this incident seriously and we would like to share information about the incident, our response, and resources available to help protect your information, should you feel it appropriate to do so.

What Happened? On March 13, 2022, ETCH identified unusual activity on its network. We promptly began taking steps to secure our systems and commenced a comprehensive investigation into the incident. Through the investigation, on March 18, 2022, we determined that certain documents stored within ETCH's environment may have been copied from or viewed on the system by an unauthorized person(s) between March 11, 2022, and March 14, 2022. We then undertook a comprehensive review of the affected data to determine what records were present and to whom the information related. You are receiving this notice because, on April 19, 2022, the investigation determined that certain information related to you was present in the affected data.

What Information Was Involved? Our investigation determined that the affected information may include your name and contact information, and includes your <<Information Affected>>.

What We Are Doing. Along with providing outstanding patient care, the confidentiality, privacy, and security of information within our care are among our highest priorities. Upon identifying this incident, we promptly took steps to secure our systems and investigate the full scope of the event. We are also reviewing and strengthening our existing policies, procedures, and safeguards related to cyber security and have already taken additional steps to further enhance the security of our systems. We have notified federal law enforcement of this incident, as well as appropriate state and federal regulators.

As an added precaution, as part of this notice, we are providing you with access to xx months of credit monitoring and identity theft protection services at no cost to you. Information on the services and instructions on how to enroll may be found in the attach ***Steps You Can Take to Protect Personal Information***.

What You Can Do. We encourage you to remain vigilant against incidents of identity theft and fraud by reviewing account statements, explanation of benefits, and monitoring free credit reports for suspicious activity and to detect errors. We also encourage you to review and consider the information and resources outlined in the attached ***Steps You Can Take to Protect Personal Information***, and to enroll in the complimentary credit monitoring and identity theft protection services we are offering. Please note, we are unable to enroll you in these services, so you will need to follow the instructions below in order to do so.

For More Information. We understand that you may have questions that are not addressed in this letter. If you have any additional questions, please call our dedicated assistance line at 1-833-749-1685 Monday through Friday, from 9:00am – 9:00pm EDT, excluding major holidays.

We apologize for any inconvenience or concern this incident may cause, and we are appreciative to the community for trusting us with the healthcare of our children. Thank you for your patience, understanding, and partnership during your continuum of care and during this incident.

Sincerely,

Matt C. Schaefer
President & Chief Executive Officer
East Tennessee Children's Hospital
2018 W. Clinch Ave, Knoxville, TN 37916

STEPS YOU CAN TAKE TO PROTECT PERSONAL INFORMATION

Enroll in Credit Monitoring

Website and Enrollment. Go to https://response.idx.us/etch and follow the instructions for enrollment using your Enrollment Code provided at the top of the letter. Please note the deadline to enroll is **August 19, 2022**.

Telephone. Contact IDX at 1-833-749-1685 to gain additional information about this event and speak with knowledgeable representatives about the appropriate steps to take to protect your credit identity.

Watch for Suspicious Activity. If you discover any suspicious items and have enrolled in IDX identity protection, notify them immediately by calling or by logging into the IDX website and filing a request for help.

If you file a request for help or report suspicious activity, you will be contacted by a member of our ID Care team who will help you determine the cause of the suspicious items. In the unlikely event that you fall victim to identity theft, you will be assigned an ID Care Specialist who will work on your behalf to identify, stop and reverse the damage quickly.

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

Monitor Your Accounts

Under U.S. law, a consumer is entitled to one free credit report annually from each of the three major credit reporting bureaus, Equifax, Experian, and TransUnion. To order your free credit report, visit www.annualcreditreport.com or call, toll-free, 1-877-322-8228. You may also directly contact the three major credit reporting bureaus listed below to request a free copy of your credit report.

Consumers have the right to place an initial or extended "fraud alert" on a credit file at no cost. An initial fraud alert is a 1-year alert that is placed on a consumer's credit file. Upon seeing a fraud alert display on a consumer's credit file, a business is required to take steps to verify the consumer's identity before extending new credit. If you are a victim of identity theft, you are entitled to an extended fraud alert, which is a fraud alert lasting seven years. Should you wish to place a fraud alert, please contact any one of the three major credit reporting bureaus listed below.

As an alternative to a fraud alert, consumers have the right to place a "credit freeze" on a credit report, which will prohibit a credit bureau from releasing information in the credit report without the consumer's express authorization. The credit freeze is designed to prevent credit, loans, and services from being approved in your name without your consent. However, you should be aware that using a credit freeze to take control over who gets access to the personal and financial information in your credit report may delay, interfere with, or prohibit the timely approval of any subsequent request or application you make regarding a new loan, credit, mortgage, or any other account involving the extension of credit. Pursuant to federal law, you cannot be charged to place or lift a credit freeze on your credit report. To request a security freeze, you will need to provide the following information:

1. Full name (including middle initial as well as Jr., Sr., II, III, etc.);
2. Social Security number;
3. Date of birth;
4. Addresses for the prior two to five years;
5. Proof of current address, such as a current utility bill or telephone bill;
6. A legible photocopy of a government-issued identification card (state driver's license or ID card, etc.); and
7. A copy of either the police report, investigative report, or complaint to a law enforcement agency concerning identity theft if you are a victim of identity theft.

SEQ
CODE 2D

Should you wish to place a credit freeze, please contact the three major credit reporting bureaus listed below:

Equifax	Experian	TransUnion
https://www.equifax.com/personal/credit-report-services/	https://www.experian.com/help/	https://www.transunion.com/credit-help
888-298-0045	1-888-397-3742	833-395-6938
Equifax Fraud Alert, P.O. Box 105069 Atlanta, GA 30348-5069	Experian Fraud Alert, P.O. Box 9554, Allen, TX 75013	TransUnion Fraud Alert, P.O. Box 2000, Chester, PA 19016
Equifax Credit Freeze, P.O. Box 105788 Atlanta, GA 30348-5788	Experian Credit Freeze, P.O. Box 9554, Allen, TX 75013	TransUnion Credit Freeze, P.O. Box 160, Woodlyn, PA 19094

Additional Information

You may further educate yourself regarding identity theft, fraud alerts, credit freezes, and the steps you can take to protect your personal information by contacting the consumer reporting bureaus, the Federal Trade Commission, or your state Attorney General. The Federal Trade Commission may be reached at: 600 Pennsylvania Avenue NW, Washington, DC 20580; www.identitytheft.gov; 1-877-ID-THEFT (1-877-438-4338); and TTY: 1-866-653-4261. The Federal Trade Commission also encourages those who discover that their information has been misused to file a complaint with them. You can obtain further information on how to file such a complaint by way of the contact information listed above. You have the right to file a police report if you ever experience identity theft or fraud. Please note that in order to file a report with law enforcement for identity theft, you will likely need to provide some proof that you have been a victim. Instances of known or suspected identity theft should also be reported to law enforcement and your state Attorney General. This notice has not been delayed by law enforcement.

For District of Columbia residents, the District of Columbia Attorney General may be contacted at: 400 6th Street, NW, Washington, DC 20001; 202-727-3400; and oag@dc.gov.

For Maryland residents, the Maryland Attorney General may be contacted at: 200 St. Paul Place, 16th Floor, Baltimore, MD 21202; 1-410-528-8662 or 1-888-743-0023; and www.oag.state.md.us.

For New Mexico residents, you have rights pursuant to the Fair Credit Reporting Act, such as the right to be told if information in your credit file has been used against you, the right to know what is in your credit file, the right to ask for your credit score, and the right to dispute incomplete or inaccurate information. Further, pursuant to the Fair Credit Reporting Act, the consumer reporting bureaus 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 credit reports to be provided to employers; you may limit "prescreened" offers of credit and insurance you get based on information in your credit report; and you may seek damages from violator. You may have additional rights under the Fair Credit Reporting Act not summarized here. Identity theft victims and active duty military personnel have specific additional rights pursuant to the Fair Credit Reporting Act. We encourage you to review your rights pursuant to the Fair Credit Reporting Act by visiting www.consumerfinance.gov/f/201504_cfpb_summary_your-rights-under-fcra.pdf, or by writing Consumer Response Center, Room 130-A, Federal Trade Commission, 600 Pennsylvania Ave. N.W., Washington, D.C. 20580.

For New York residents, the New York Attorney General may be contacted at: Office of the Attorney General, The Capitol, Albany, NY 12224-0341; 1-800-771-7755; or https://ag.ny.gov/.

For North Carolina residents, the North Carolina Attorney General may be contacted at: 9001 Mail Service Center, Raleigh, NC 27699-9001; 1-877-566-7226 or 1-919-716-6000; and www.ncdoj.gov.

For Rhode Island residents, the Rhode Island Attorney General may be reached at: 150 South Main Street, Providence, RI 02903; www.riag.ri.gov; and 1-401-274-4400. Under Rhode Island law, you have the right to obtain any police report filed in regard to this incident. There are xx Rhode Island residents impacted by this incident.

EXHIBIT B

NOTICE OF DATA INCIDENT

ABOUT THE DATA INCIDENT

East Tennessee Children's Hospital ("ETCH") is making individuals aware of a recent incident that may affect the privacy of certain information. ETCH takes this incident and the privacy of information in its care very seriously. While the investigation into this incident is ongoing, ETCH is providing notice of the event so that potentially affected individuals may take steps to better protect their information from misuse, should they feel it appropriate to do so.

FREQUENTLY ASKED QUESTIONS

What Happened? On March 13, 2022, ETCH identified unusual activity on its network. We promptly began taking steps to secure our systems and commenced a comprehensive investigation into the incident. Through the investigation to date, we have determined that ETCH experienced a cyber incident. While our investigation is ongoing, on March 18, 2022, we determined that certain documents stored within ETCH's environment may have been copied from or viewed on the system as part of the cyber incident between March 11, 2022 – March 14, 2022. Based on the investigation, ETCH is currently working to determine the scope of potentially affected information and conducting a detailed review of the potentially impacted data to determine the type of information present and to whom it relates. This effort is currently ongoing.

What Information Was Involved? While the investigation to determine the full scope of potentially affected information is ongoing and may vary by individual, the relevant ETCH systems may contain the following types of information at the time of the event: names, date of birth, Social Security number, driver's license or state identification number, non-resident identification number, other demographic information, medical information, health insurance information, credit or debit card information, financial information, billing information, other personal health information, and usernames and passwords.

What is ETCH Doing? Along with providing outstanding patient care, the confidentiality, privacy, and security of information within our care are among our highest priorities. Upon discovering this incident, we promptly took steps to secure our systems and investigate the full scope of the incident. While the investigation of and response to the event are ongoing, we have taken additional steps to further enhance the security of our systems. As our investigation continues, we will also be notifying potentially affected individuals and providing information on steps that may be taken to best protect personal information.

What You Can Do? We encourage potentially affected individuals to remain vigilant against incidents of identity theft and fraud by reviewing account statements, explanation of benefits, and monitoring free credit reports for suspicious activity and to detect errors. Individuals may also review and consider the information and resources outlined in the *Steps Individuals Can Take to Protect Their Personal Information* found below.

For More Information. If individuals have additional questions about this incident, they may contact our assistance line at1-833-749-1685, Monday through Friday, from –9:00am – 9:00pm EDT, excluding major U.S. holidays.

STEPS INDIVIDUALS CAN TAKE TO PROTECT THEIR PERSONAL INFORMATION

Monitor Your Accounts by:

1. **Requesting a Free Credit Report**

   Under U.S. law, a consumer is entitled to one free credit report annually from each of the three major credit reporting bureaus, Equifax, Experian, and TransUnion. To order your free credit report, visit www.annualcreditreport.com or call, toll-free, 1-877-322-8228.

2. **Placing a "Fraud Alert" on Your Credit File**

   Consumers have the right to place an initial or extended "fraud alert" on a credit file at no cost. An initial fraud alert is a 1-year alert that is placed on a consumer's credit file. Upon seeing a fraud alert display on a consumer's credit file, a business is required to take steps to verify the consumer's identity before extending new credit. If you are a victim of identity theft, you are entitled to an extended fraud alert, which is a fraud alert lasting seven years. Should you wish to place a fraud alert, please contact any one of the three major credit reporting bureaus listed below.

3. **Placing a "Credit Freeze" on a Credit Report**

   As an alternative to a fraud alert, consumers have the right to place a "credit freeze" on a credit report, which will prohibit a credit bureau from releasing information in the credit report without the consumer's express authorization. The credit freeze is designed to prevent credit, loans, and services from being approved in your name without your consent. However, you should be aware that using a credit freeze to take control over who gets access to the personal and financial information in your credit report may delay, interfere with, or prohibit the timely approval of any subsequent request or application you make regarding a new loan, credit, mortgage, or any other account involving the extension of credit. Pursuant to federal law, you cannot be charged to place or lift a credit freeze on your credit report. To request a credit freeze, you will need to provide the following information:

   1. Full name (including middle initial as well as Jr., Sr., II, III, etc.);
   2. Social Security number;
   3. Date of birth;
   4. Addresses for the prior two to five years;
   5. Proof of current address, such as a current utility bill or telephone bill;
   6. A legible photocopy of a government-issued identification card (state driver's license or ID card, etc.); and
   7. A copy of either the police report, investigative report, or complaint to a law enforcement agency concerning identity theft if you are a victim of identity theft.

Should you wish to place a credit freeze, please contact the three major credit reporting bureaus listed below:

Equifax	Experian	TransUnion
https://www.equifax.com/personal/credit-report-services/	https://www.experian.com/help/	https://www.transunion.com/credit-help
1-888-298-0045	1-888-397-3742	833-395-6938
Equifax Fraud Alert, P.O. Box 105069 Atlanta, GA 30348-5069	Experian Fraud Alert, P.O. Box 9554, Allen, TX 75013	TransUnion Fraud Alert, P.O. Box 2000, Chester, PA 19016
Equifax Credit Freeze, P.O. Box 105788 Atlanta, GA 30348-5788	Experian Credit Freeze, P.O. Box 9554, Allen, TX 75013	TransUnion Credit Freeze, P.O. Box 160, Woodlyn, PA 19094

Additional Information

For more information regarding identity theft, fraud alerts, credit freezes, and the steps you can take to protect your personal information by contacting the consumer reporting bureaus, the Federal Trade Commission, or your state Attorney General. The Federal Trade Commission may be reached at: 600 Pennsylvania Avenue NW, Washington, DC 20580; www.identitytheft.gov; 1-877-ID-THEFT (1-877-438-4338); and TTY: 1-866-653-4261. The Federal Trade Commission also encourages those who discover that their information has been misused to file a complaint with them. You can obtain further information on how to file such a complaint by way of the contact information listed above. You have the right to file a police report if you ever experience identity theft or fraud. Please note that in order to file a report with law enforcement for identity theft, you will likely need to provide some proof that you have been a victim. Instances of known or suspected identity theft should also be reported to law enforcement and your state Attorney General. This notice has not been delayed by law enforcement.

For District of Columbia residents, the District of Columbia Attorney General may be contacted at: 400 6th Street, NW, Washington, DC 20001; 202-727-3400; and oag@dc.gov.

For Maryland residents, the Maryland Attorney General may be contacted at: 200 St. Paul Place, 16th Floor, Baltimore, MD 21202; 1-410-528-8662 or 1-888-743-0023; and www.oag.state.md.us. ETCH is located at 2018 W. Clinch Ave., Knoxville, TN 37916.

For New Mexico residents, you have rights pursuant to the Fair Credit Reporting Act, such as the right to be told if information in your credit file has been used against you, the right to know what is in your credit file, the right to ask for your credit score, and the right to dispute incomplete or inaccurate information. Further, pursuant to the Fair Credit Reporting Act, the consumer reporting bureaus 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 credit reports to be provided to employers; you may limit "prescreened" offers of credit and insurance you get based on information in your credit report; and you may seek damages from violator. You may have additional rights under the Fair Credit Reporting Act not summarized here. Identity theft victims and active duty military personnel have specific additional rights pursuant to the Fair Credit Reporting Act. We encourage you to review your rights pursuant to the Fair Credit Reporting Act by visiting www.consumerfinance.gov/f/201504_cfpb_summary_your-rights-under-fcra.pdf, or by writing Consumer Response Center, Room 130-A, Federal Trade Commission, 600 Pennsylvania Ave. N.W., Washington, D.C. 20580.

For New York residents, the New York Attorney General may be contacted at: Office of the Attorney General, The Capitol, Albany, NY 12224-0341; 1-800-771-7755; or https://ag.ny.gov/.

For North Carolina residents, the North Carolina Attorney General may be contacted at: 9001 Mail Service Center, Raleigh, NC 27699-9001; 1-877-566-7226 or 1-919-716-6000; and www.ncdoj.gov.

For Rhode Island residents, the Rhode Island Attorney General may be reached at: 150 South Main Street, Providence, RI 02903; www.riag.ri.gov; and 1-401-274-4400. Under Rhode Island law, you have the right to obtain any police report filed in regard to this incident. To date, the number of Rhode Island residents potentially impacted by this incident, if any, is unknown.

EXHIBIT C

EAST TENNESSEE CHILDREN'S HOSPITAL PROVIDES NOTICE OF A DATA INCIDENT

Knoxville, TN – April 7, 2022. East Tennessee Children's Hospital ("ETCH") is providing notice of a recent incident that may affect the privacy of certain information. ETCH takes this incident and the privacy of information in its care very seriously. While the investigation into this incident is ongoing, ETCH is providing notice of the event so that potentially affected individuals may take steps to better protect their information from misuse, should they feel it appropriate to do so.

What Happened? On March 13, 2022, ETCH identified unusual activity on its network. ETCH promptly began taking steps to secure its systems and commenced a comprehensive investigation into the incident. Through the investigation to date, ETCH has determined that it experienced a cyber incident. While the investigation is ongoing, on March 18, 2022, ETCH determined that certain documents stored within its environment may have been copied from or viewed on the system as part of the cyber incident between March 11, 2022 – March 14, 2022. Based on the investigation, ETCH is currently working to determine the scope of potentially affected information and conducting a detailed review of the potentially impacted data to determine the type of information present and to whom it relates. This effort is currently ongoing.

What Information Was Involved? While the investigation to determine the full scope of potentially affected information is ongoing and may vary by individual, the relevant ETCH systems may contain the following types of information at the time of the event: names, date of birth, Social Security number, driver's license or state identification number, non-resident identification number, other demographic information, medical information, health insurance information, credit or debit card information, financial information, billing information, other personal health information, and usernames and passwords.

What is ETCH Doing? Along with providing outstanding patient care, the confidentiality, privacy, and security of information within its care are among ETCH's highest priorities. Upon discovering this incident, ETCH promptly took steps to secure its systems and investigate the full scope of the incident. While the investigation of and response to the event are ongoing, ETCH has taken additional steps to further enhance the security of its systems. As the investigation continues, ETCH will also be notifying potentially affected individuals and providing information on steps that may be taken to best protect personal information.

What You Can Do? ETCH is encouraging potentially affected individuals to remain vigilant against incidents of identity theft and fraud by reviewing account statements, explanation of benefits, and monitoring free credit reports for suspicious activity and to detect errors. Individuals may also review and consider the information and resources outlined in the *Steps Individuals Can Take to Protect Their Personal Information*, which may be found below and on ETCH's website at https://www.etch.com/.

For More Information. If individuals have additional questions about this incident, they may contact ETCH's assistance line at 1-833-749-1685, Monday through Friday, from 9:00am – 9:00pm EDT, excluding major U.S. holidays.

STEPS INDIVIDUALS CAN TAKE TO PROTECT THEIR PERSONAL INFORMATION

Monitor Your Accounts by:

1. **Requesting a Free Credit Report**

Under U.S. law, a consumer is entitled to one free credit report annually from each of the three major credit reporting bureaus, Equifax, Experian, and TransUnion. To order your free credit report, visit www.annualcreditreport.com or call, toll-free, 1-877-322-8228.

2. **Placing a "Fraud Alert" on Your Credit File**

Consumers have the right to place an initial or extended "fraud alert" on a credit file at no cost. An initial fraud alert is a 1-year alert that is placed on a consumer's credit file. Upon seeing a fraud alert display on a consumer's credit file, a business is required to take steps to verify the consumer's identity before extending new credit. If you are a victim of identity theft, you are entitled to an extended fraud alert, which is a fraud alert lasting seven years. Should you wish to place a fraud alert, please contact any one of the three major credit reporting bureaus listed below.

3. **Placing a "Credit Freeze" on a Credit Report**

As an alternative to a fraud alert, consumers have the right to place a "credit freeze" on a credit report, which will prohibit a credit bureau from releasing information in the credit report without the consumer's express authorization. The credit freeze is designed to prevent credit, loans, and services from being approved in your name without your consent. However, you should be aware that using a credit freeze to take control over who gets access to the personal and financial information in your credit report may delay, interfere with, or prohibit the timely approval of any subsequent request or application you make regarding a new loan, credit, mortgage, or any other account involving the extension of credit. Pursuant to federal law, you cannot be charged to place or lift a credit freeze on your credit report. To request a credit freeze, you will need to provide the following information:

1. Full name (including middle initial as well as Jr., Sr., II, III, etc.);
2. Social Security number;
3. Date of birth;
4. Addresses for the prior two to five years;
5. Proof of current address, such as a current utility bill or telephone bill;
6. A legible photocopy of a government-issued identification card (state driver's license or ID card, etc.); and
7. A copy of either the police report, investigative report, or complaint to a law enforcement agency concerning identity theft if you are a victim of identity theft.

Should you wish to place a credit freeze, please contact the three major credit reporting bureaus listed below:

Equifax	**Experian**	**TransUnion**
https://www.equifax.com/personal/credit-report-services/	https://www.experian.com/help/	https://www.transunion.com/credit-help
1-888-298-0045	1-888-397-3742	833-395-6938
Equifax Fraud Alert, P.O. Box 105069 Atlanta, GA 30348-5069	Experian Fraud Alert, P.O. Box 9554, Allen, TX 75013	TransUnion Fraud Alert, P.O. Box 2000, Chester, PA 19016

Equifax Credit Freeze, P.O. Box 105788 Atlanta, GA 30348-5788	Experian Credit Freeze, P.O. Box 9554, Allen, TX 75013	TransUnion Credit Freeze, P.O. Box 160, Woodlyn, PA 19094

Additional Information

For more information regarding identity theft, fraud alerts, credit freezes, and the steps you can take to protect your personal information by contacting the consumer reporting bureaus, the Federal Trade Commission, or your state Attorney General. The Federal Trade Commission may be reached at: 600 Pennsylvania Avenue NW, Washington, DC 20580; www.identitytheft.gov; 1-877-ID-THEFT (1-877-438-4338); and TTY: 1-866-653-4261. The Federal Trade Commission also encourages those who discover that their information has been misused to file a complaint with them. You can obtain further information on how to file such a complaint by way of the contact information listed above. You have the right to file a police report if you ever experience identity theft or fraud. Please note that in order to file a report with law enforcement for identity theft, you will likely need to provide some proof that you have been a victim. Instances of known or suspected identity theft should also be reported to law enforcement and your state Attorney General. This notice has not been delayed by law enforcement.

For District of Columbia residents, the District of Columbia Attorney General may be contacted at: 400 6th Street, NW, Washington, DC 20001; 202-727-3400; and oag@dc.gov.

For Maryland residents, the Maryland Attorney General may be contacted at: 200 St. Paul Place, 16th Floor, Baltimore, MD 21202; 1-410-528-8662 or 1-888-743-0023; and www.oag.state.md.us. ETCH is located at 2018 W. Clinch Ave., Knoxville, TN 37916.

For New Mexico residents, you have rights pursuant to the Fair Credit Reporting Act, such as the right to be told if information in your credit file has been used against you, the right to know what is in your credit file, the right to ask for your credit score, and the right to dispute incomplete or inaccurate information. Further, pursuant to the Fair Credit Reporting Act, the consumer reporting bureaus 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 credit reports to be provided to employers; you may limit "prescreened" offers of credit and insurance you get based on information in your credit report; and you may seek damages from violator. You may have additional rights under the Fair Credit Reporting Act not summarized here. Identity theft victims and active duty military personnel have specific additional rights pursuant to the Fair Credit Reporting Act. We encourage you to review your rights pursuant to the Fair Credit Reporting Act by visiting www.consumerfinance.gov/f/201504_cfpb_summary_your-rights-under-fcra.pdf, or by writing Consumer Response Center, Room 130-A, Federal Trade Commission, 600 Pennsylvania Ave. N.W., Washington, D.C. 20580.

For New York residents, the New York Attorney General may be contacted at: Office of the Attorney General, The Capitol, Albany, NY 12224-0341; 1-800-771-7755; or https://ag.ny.gov/.

For North Carolina residents, the North Carolina Attorney General may be contacted at: 9001 Mail Service Center, Raleigh, NC 27699-9001; 1-877-566-7226 or 1-919-716-6000; and www.ncdoj.gov.

For Rhode Island residents, the Rhode Island Attorney General may be reached at: 150 South Main Street, Providence, RI 02903; www.riag.ri.gov; and 1-401-274-4400. Under Rhode Island law, you have the right

to obtain any police report filed in regard to this incident. To date, the number of Rhode Island residents potentially impacted by this incident, if any, is unknown.