WOODS ROGERS VANDEVENTER BLACK
ATTORNEYS AT LAW

CHRISTINE S. WARD
(540) 983-7522
Christine.Ward@wrvblaw.com

January 18, 2024

Washington Attorney General's Office
PO Box 40100
Olympia, WA 98504

To Whom It May Concern:

Pursuant to RCW 42.56.590(7), I am writing on behalf of my client, the Washington Center for Deaf & Hard of Hearing Youth ("CDHY"), to notify you regarding the nature and circumstances of a recent data security incident. CDHY's mailing address is 611 Grand Blvd, S-26, Vancouver, WA 98661.

On December 16, 2023, CDHY discovered disruptions to certain computer systems and, shortly thereafter, determined it was the victim of a sophisticated ransomware incident that began on approximately December 14, 2023. As part of the incident response, my firm engaged leading outside cybersecurity experts to assist in the investigation and remediation of these issues. Thankfully the impact to operations, including school services, was limited and CDHY was able to continue offering educational services with minimal disruptions. However, we determined that certain computer servers holding sensitive information may have been inappropriately accessed by cyber criminals during the ransomware incident.

CDHY immediately began identifying the names and addresses of its students and employees to provide notice to the community it serves. The cyber criminals might have been able to access one or more of the following types of information: Social Security number; date of birth; driver's license or state employee number; student, military, or passport identification number; health insurance policy number or health insurance identification number; or information about medical history, diagnosis, or treatment.

CDHY has notified federal and state law enforcement of this incident, including the FBI Cyber Crimes Division and the Washington State Patrol, and intends to support any law enforcement investigation. Additionally, CDHY has secured the services of Kroll to provide 12 months of identity monitoring services at no cost to its students and employees.

On January 16, 2024, CDHY mailed its current students and employees, including 284 Washington residents, notifications concerning this incident. More notifications will be mailed to 310 former CDHY employees and students later this week. While our mailing vendor is still confirming the final date for the second mailing, when it goes out, we will have notified 594 Washington residents about this incident in total. For your reference, sample copies of the letters are attached.

If you have any questions, please do not hesitate to contact me.

Very truly yours,

Christine Ward
Woods Rogers Vandeventer Black

Enclosures

STATE OF WASHINGTON
WASHINGTON CENTER FOR
DEAF and HARD of HEARING YOUTH

611 Grand Blvd., S-26 Vancouver, Washington 98661-4918 • (360) 696-6525
Administration FAX (360) 696-6291 • Business Office FAX (360) 418-0418

<<Date>> (Format: Month Day, Year)

<<first_name>> <<middle_name>> <<last_name>> <<suffix>>
<<address_1>>
<<address_2>>
<<city>>, <<state_province>> <<postal_code>>
<<country>>

Dear <<first_name>> <<middle_name>> <<last_name>> <<suffix>>,

The Washington Center for Deaf & Hard of Hearing Youth ("CDHY"), like many organizations across the country, has unfortunately been the victim of cybersecurity incident. We are writing to share with you how this incident may have affected your personal information and, as a preventative measure, to provide you with steps you can take to help protect your information. CDHY takes the privacy and security of your personal information very seriously and we sincerely regret any concern this incident may cause you.

What Happened

On December 16, 2023, we discovered disruptions to certain computer systems and, shortly thereafter, determined we were the victim of a sophisticated ransomware incident that began on approximately December 14, 2023. In a ransomware incident, cyber criminals attempt to encrypt or lock up data and, in some cases, try to steal data from an organization. Thankfully the impact to our operations, including our school services, was limited and we were able to continue forward with our educational services with minimal disruptions.

As part of our incident response, we engaged leading outside cybersecurity experts to assist in the investigation and remediation of these issues. Those professionals determined that certain computer servers holding sensitive information may have been inappropriately accessed by cyber criminals during the ransomware incident. We immediately began identifying the names and addresses of all our current employees to provide notice to the community we serve so that you would be aware of these issues and be able to take steps to help protect your personal information.

What Information Was Involved?

We have determined that the information accessed in this incident may include your personal information that we use as a part of your employment relationship with us. In particular, the information involved may include one or more of the following types of information: Social Security number; date of birth; driver's license or state employee number; military or passport identification number; health insurance policy number or health insurance identification number; or information about your medical history, diagnosis, or treatment that would have been provided to us as a part of your ongoing employment. We are not certain that all of the above categories of information were accessed by the cyber criminals; however, we wanted to make you aware of these issues and the possible impact of this incident.

What We Are Doing

We have notified federal and state law enforcement of this incident, including the FBI Cyber Crimes Division and the Washington State Police, and intend to support any law enforcement investigation. Upon discovering the incident, as noted above, we began an investigation and engaged leading outside cybersecurity experts to confirm the scope of this incident and to take measures to further protect our systems from unauthorized access. We take our obligation to safeguard personal information very seriously and are continuing to evaluate additional actions to strengthen our network security in the face of ever-evolving cybersecurity threats.

To relieve concerns and restore confidence following this incident, we have secured the services of Kroll to provide identity monitoring at no cost to you for **12 months**. Kroll is a global leader in identity risk mitigation and response, and its team has extensive experience helping people who have sustained an unintentional exposure of confidential data. Your identity monitoring services include Credit Monitoring, Fraud Consultation, and Identity Theft Restoration. Details on accessing this information are included with this letter.

What You Can Do

Please review the enclosed "Additional Resources" section included with this letter. This section describes additional steps you can take to help protect yourself, including recommendations from the Federal Trade Commission regarding identity theft protection and details on how to place a fraud alert or a security freeze on your credit file.

For More Information

You will be able to access an American Sign Language interpreted version of this letter in the near future. We will provide the link in an All-Staff email. If you have any further questions regarding this matter or the identity monitoring services provided, please call **<<KROLL TFN>>**, Monday through Friday from 9:00 a.m. to 6:30 p.m. Eastern Time, excluding major U.S. holidays. Please have your Membership Number ready: **<<Membership Number s_n>>**. Please also note that CDHY is utilizing Kroll's return mail service, so the return address on this letter is to Kroll's mailing center.

We deeply regret that this incident occurred and are committed to supporting you.

Sincerely,

Shauna Bilyeu
Interim Executive Director
Center for Deaf and Hard of Hearing Youth
Washington School for the Deaf

ADDITIONAL RESOURCES

KROLL

We have secured the services of Kroll to provide identity monitoring at no cost to you for 12 months. Kroll is a global leader in risk mitigation and response, and their team has extensive experience helping people who have sustained an unintentional exposure of confidential data. Your identity monitoring services[1] include Credit Monitoring, Fraud Consultation, and Identity Theft Restoration.

How to Activate Your Identity Monitoring Services

Visit **https://enroll.krollmonitoring.com** to activate and take advantage of your identity monitoring services.

You have until <<b2b_text_6(activation deadline)>> to activate your identity monitoring services.

Membership Number: **<<Membership Number s_n>>**

For more information about Kroll and your Identity Monitoring services, you can visit info.krollmonitoring.com.

Take Advantage of Your Identity Monitoring Services

You've been provided with access to the following services[1] from Kroll:

Single Bureau Credit Monitoring

You will receive alerts when there are changes to your credit data—for instance, when a new line of credit is applied for in your name. If you do not recognize the activity, you'll have the option to call a Kroll fraud specialist, who can help you determine if it's an indicator of identity theft.

Fraud Consultation

You have unlimited access to consultation with a Kroll fraud specialist. Support includes showing you the most effective ways to protect your identity, explaining your rights and protections under the law, assistance with fraud alerts, and interpreting how personal information is accessed and used, including investigating suspicious activity that could be tied to an identity theft event.

Identity Theft Restoration

If you become a victim of identity theft, an experienced Kroll licensed investigator will work on your behalf to resolve related issues. You will have access to a dedicated investigator who understands your issues and can do most of the work for you. Your investigator can dig deep to uncover the scope of the identity theft, and then work to resolve it.

STEPS YOU CAN TAKE TO FURTHER HELP PROTECT YOUR INFORMATION

Review Your Account Statements and Obtain and Monitor Your Credit Report

As a precautionary measure, we recommend that you remain vigilant by regularly reviewing and monitoring account statements and credit reports to detect potential errors or fraud and identity theft resulting from the security incident. You may periodically obtain your free 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	**Experian**	**TransUnion**
P.O. Box 740241	P.O. Box 9701	P.O. Box 1000
Atlanta, GA 30374-0241	Allen, TX 75013-9701	Chester, PA 19016-1000
1-800-685-1111	1-888-397-3742	1-800-916-8800
www.equifax.com	www.experian.com	www.transunion.com

When you receive your credit reports, review them carefully. Look for accounts or creditor inquiries that you did not initiate or do not recognize. Look for inaccurate information, such as a home address and Social Security number. If you see anything you do not understand, call the credit reporting agency at the telephone number on the report.

[1] Kroll's activation website is only compatible with the current version or one version earlier of Chrome, Firefox, Safari, and Edge. To receive credit services, you must be over the age of 18 and have established credit in the U.S., have a Social Security number in your name, and have a U.S. residential address associated with your credit file.

Notify Law Enforcement of Suspicious Activity

You should promptly report any fraudulent activity or any suspected incidence of identity theft to proper law enforcement authorities, including local law enforcement, your state attorney general, and the Federal Trade Commission (FTC). To file a complaint with the FTC, use the below contact information or website.

The Federal Trade Commission
600 Pennsylvania Avenue, NW
Washington, DC 20580
1-877-ID-THEFT (1-877-438-4338)
TTY: 1-866-653-4261
www.IdentityTheft.gov

Complaints filed with the FTC will be added to the FTC's Identity Theft Data Clearinghouse, which is a database made available to law enforcement agencies. If you detect any suspicious activity on an account, you should promptly notify the financial institution or company which the account is maintained.

Credit Freezes

You have the right to put a security freeze, also known as a credit freeze, on your credit file, so that no new credit can be opened in your name without the use of a Personal Identification Number (PIN) that is issued when you initiate a freeze. A credit freeze is designed to prevent potential creditors from accessing your credit report without your consent. If you place a credit freeze, potential creditors and other third parties will not be able to access your credit report unless you temporarily lift the freeze. Therefore, using a credit freeze may delay your ability to obtain credit. Pursuant to federal law, you cannot be charged to place or lift a credit freeze on your credit report. Should you wish to place a credit freeze, please contact **all three** major consumer reporting agencies listed below.

Equifax	**Experian**	**TransUnion**
P.O. Box 105788	P.O. Box 9554	P.O. Box 2000
Atlanta, GA 30348-5788	Allen, TX 75013-9554	Chester, PA 19016-2000
1-800-685-1111	1-888-397-3742	1-800-916-8800
www.equifax.com/personal/credit-report-services	www.experian.com/freeze/center.html	www.transunion.com/credit-freeze

You must separately place a credit freeze on your credit file at each credit reporting agency. The following information should be included when requesting a credit freeze:

1. Your full name, with middle initial and any suffixes;
2. Your Social Security number;
3. Your date of birth (month, day, and year);
4. Your current address and previous addresses for the past five (5) years;
5. A copy of your state-issued identification card (such as a state driver's license or military ID);
6. Proof of your current residential address (such as a current utility bill or account statement); and
7. Other personal information as required by the applicable credit reporting agency.

If you request a credit freeze online or by phone, then the credit reporting agencies have one (1) business day after receiving your request to place a credit freeze on your credit file report. If you request a lift of the credit freeze online or by phone, then the credit reporting agency must lift the freeze within one (1) hour. If you request a credit freeze or lift of a credit freeze by mail, then the credit agency must place or lift the credit freeze no later than three (3) business days after getting your request. More information regarding credit freezes can be obtained from the FTC and the major consumer reporting agencies.

Fraud Alerts

You also have the right to place an initial or extended fraud alert on your file at no cost. An initial fraud alert will stay on your credit file one (1) year. The alert informs creditors of possible fraudulent activity within your report and requires the creditor to verify your 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 7 years. Should you wish to place a fraud alert, please contact any one of the three major consumer reporting agencies listed above. The agency you contact will then contact the other two. More information regarding fraud alerts can be obtained from the FTC and the major consumer reporting agencies.

Monitor Your Personal Health Information

If applicable to your situation, 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 the 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 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 records.

Additional Resources and Information

You can obtain additional information and further educate yourself regarding identity theft and the steps you can take to protect yourself by contacting your state attorney general or the FTC. The FTC's contact information and website for additional information is:

The Federal Trade Commission
600 Pennsylvania Avenue, NW
Washington, DC 20580
1-877-ID-THEFT (1-877-438-4338)
TTY: 1-866-653-4261
www.ftc.gov/idtheft

For Connecticut residents: You may contact the Connecticut Office of the Attorney General at 165 Capitol Avenue, Hartford, CT 06106; 1-860-808-5318; or https://portal.ct.gov/ag.

For District of Columbia residents: You may contact the Office of the Attorney General for the District of Columbia at 400 6th Street, NW, Washington, DC 20001; 1-202-727-3400; or https://oag.dc.gov/consumer-protection/consumer-alert-online-privacy.

For Iowa residents: You may contact law enforcement or the Iowa Attorney General's Office to report suspected incidents of identity theft. The Iowa Attorney General's Office can be reached at 1305 E. Walnut Street, Des Moines, IA 50319; 1-515-281-5164; or www.iowaattorneygeneral.gov.

For Maryland residents: You may contact the Maryland Office of the Attorney General, Consumer Protection Division, 200 St. Paul Place, Baltimore, MD 21202; 410-576-6300; 1-888-743-0023 (toll free), or https://www.marylandattorneygeneral.gov/Pages/contactus.aspx.

For Massachusetts residents: You may contact the Office of the Massachusetts Attorney General at 1 Ashburton Place, Boston, MA 02108; 1-617-727-8400; or https://www.mass.gov/orgs/office-of-the-attorney-general. You have the right to obtain a police report if you are a victim of identity theft.

For New Mexico residents: You have rights under the federal Fair Credit Reporting Act ("FCRA"). These include, among others, the right to know what is in your credit 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

https://files.consumerfinance.gov/f/201504_cfpb_summary_your-rights-under-fcra.pdf or ww.ftc.gov.

For New York residents: The 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/. You may also contact the Bureau of Internet and Technology (BIT) at 28 Liberty Street, New York, NY 10005; 212-416-8433l; or https://ag.ny.gov/about/about-office/economic-justice-division#internet-technology.

For North Carolina residents: The North Carolina Attorney General's Office may be contacted at 9001 Mail Service Center, Raleigh, NC 27699-9001; 919-716-6400; or https://ncdoj.gov/contact-doj/.

For Oregon residents: We encourage you to report suspected identity theft to the Oregon Attorney General at 1162 Court Street NE, Salem, OR 97301; 1-877-877-9392; 1-503-378-4400; or www.doj.state.or.us.

For Rhode Island residents: You may contact the Rhode Island Office of the Attorney General at 150 South Main Street, Providence, RI 02903; 1-401-274-4400; or https://riag.ri.gov/. You have the right to obtain a police report if you are a victim of identity theft. No Rhode Island residents were impacted by this breach.

For Virginia residents: You may contact the Virginia Attorney General's Office at 202 North Ninth Street, Richmond, VA 23219; 1-804-786-2071; or https://www.oag.state.va.us/contact-us/contact-info.

STATE OF WASHINGTON
WASHINGTON CENTER FOR
DEAF and HARD of HEARING YOUTH

611 Grand Blvd., S-26 Vancouver, Washington 98661-4918 • (360) 696-6525
Administration FAX (360) 696-6291 • Business Office FAX (360) 418-0418

<<Date>> (Format: Month Day, Year)

Parents/Guardians of
<<first_name>> <<middle_name>> <<last_name>> <<suffix>>
<<address_1>>
<<address_2>>
<<city>>, <<state_province>> <<postal_code>>
<<country>>

Dear Parents/Guardians of <<first_name>> <<middle_name>> <<last_name>> <<suffix>>,

The Washington Center for Deaf & Hard of Hearing Youth ("CDHY"), like many organizations across the country, has unfortunately been the victim of cybersecurity incident. We are writing to share with you how this incident may have affected your student's personal information and, as a preventative measure, to provide you with steps you can take to help protect your minor's information. CDHY takes the privacy and security of your student's personal information very seriously and we sincerely regret any concern this incident may cause you.

What Happened

On December 16, 2023, we discovered disruptions to certain computer systems and, shortly thereafter, determined we were the victim of a sophisticated ransomware incident that began on approximately December 14, 2023. In a ransomware incident, cyber criminals attempt to encrypt or lock up data and, in some cases, try to steal data from an organization. Thankfully the impact to our operations, including our school services, was limited and we were able to continue forward with our educational services with minimal disruptions.

As part of our incident response, we engaged leading outside cybersecurity experts to assist in the investigation and remediation of these issues. Those professionals determined that certain computer servers holding sensitive information may have been inappropriately accessed by cyber criminals during the ransomware incident. We immediately began identifying the names and addresses of all our current students to provide notice to the community we serve so that you would be aware of these issues and be able to take steps to protect your minor's personal information.

What Information Was Involved?

We have determined that the information accessed in this incident may include your student's personal information that we use to provide educational or support services to your student. In particular, the information involved may include one or more of the following types of information: Social Security number; date of birth; driver's license or state identification card number; student, military, or passport identification number; health insurance policy number or health insurance identification number; or information about your student's medical history, diagnosis, or treatment. We are not certain that all of the above categories of information were accessed by the cyber criminals; however, we wanted to make you aware of these issues and the possible impact of this incident.

What We Are Doing

We have notified federal and state law enforcement of this incident, including the FBI Cyber Crimes Division and the Washington State Police, and intend to support any law enforcement investigation. Upon discovering the incident, as noted above, we began an investigation and engaged leading outside cybersecurity experts to confirm the scope of this incident and to take measures to further protect our systems from unauthorized access. We take our obligation to safeguard personal information very seriously and are continuing to evaluate additional actions to strengthen our network security in the face of ever-evolving cybersecurity threats.

To relieve concerns and restore confidence following this incident, we have secured the services of Kroll to provide minor identity monitoring at no cost to you for **12 months**. Kroll is a global leader in identity risk mitigation and response, and its team has extensive experience helping people who have sustained an unintentional exposure of confidential data. Your minor identity monitoring services include Minor Identity Monitoring, Fraud Consultation, and Identity Theft Restoration. Details on accessing this information are included with this letter.

What You Can Do

Please review the enclosed "Additional Resources" section included with this letter. This section describes additional steps you can take to help protect your student, including recommendations from the Federal Trade Commission regarding identity theft protection and details on how to place a fraud alert or a security freeze on your student's credit file.

For More Information

You will be able to access an American Sign Language interpreted version of this letter in the near future. We will provide the link when it is ready. If you have any further questions regarding this matter or the identity monitoring services provided, please call **<<KROLL TFN>>**, Monday through Friday from 9:00 a.m. to 6:30 p.m. Eastern Time, excluding major U.S. holidays. Please have your student's Membership Number ready: **<<Membership Number s_n>>**. Please also note that CDHY is utilizing Kroll's return mail service, so the return address on this letter is to Kroll's mailing center.

We deeply regret that this incident occurred and are committed to supporting you.

Sincerely,

Shauna Bilyeu
Interim Executive Director
Center for Deaf and Hard of Hearing Youth
Washington School for the Deaf

ADDITIONAL RESOURCES

KROLL

We have secured the services of Kroll to provide minor identity monitoring at no cost to you for 12 months. Kroll is a global leader in risk mitigation and response, and their team has extensive experience helping people who have sustained an unintentional exposure of confidential data. Your child's minor identity monitoring services include Minor Identity Monitoring, Fraud Consultation, and Identity Theft Restoration.

How to Activate Your Child's Identity Monitoring Services

Visit **https://enroll.krollmonitoring.com** to activate and take advantage of your Minor Identity Monitoring services.

You have until <<b2b_text_6(activation deadline)>> to activate your Minor Identity Monitoring services.

Membership Number: <<Membership Number s_n>>

For more information about Kroll and your Identity Monitoring services, you can visit info.krollmonitoring.com.

Take Advantage of Your Child's Identity Monitoring Services

You've child been provided with access to the following services[1] from Kroll:

Minor Identity Monitoring

Minor Identity Monitoring detects when names, addresses, and credit information is associated with your child's Social Security number. An alert will be sent to you when activity is detected. The presence of a credit file may be an indicator of identity theft or fraud for children who, as minors, should not have a credit history.

Fraud Consultation

You have unlimited access to consultation with a Kroll fraud specialist. Support includes showing you the most effective ways to protect your identity, explaining your rights and protections under the law, assistance with fraud alerts, and interpreting how personal information is accessed and used, including investigating suspicious activity that could be tied to an identity theft event.

Identity Theft Restoration

If you become a victim of identity theft, an experienced Kroll licensed investigator will work on your behalf to resolve related issues. You will have access to a dedicated investigator who understands your issues and can do most of the work for you. Your investigator can dig deep to uncover the scope of the identity theft, and then work to resolve it.

STEPS YOU CAN TAKE TO FURTHER HELP PROTECT YOUR MINOR'S INFORMATION

Review Your Account Statements and Obtain and Monitor Your Credit Report

As a precautionary measure, we recommend that you remain vigilant by regularly reviewing and monitoring account statements and credit reports to detect potential errors or fraud and identity theft resulting from the security incident. You may periodically obtain your free 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	**Experian**	**TransUnion**
P.O. Box 740241	P.O. Box 9701	P.O. Box 1000
Atlanta, GA 30374-0241	Allen, TX 75013-9701	Chester, PA 19016-1000
1-800-685-1111	1-888-397-3742	1-800-916-8800
www.equifax.com	www.experian.com	www.transunion.com

When you receive your credit reports, review them carefully. Look for accounts or creditor inquiries that you did not initiate or do not recognize. Look for inaccurate information, such as a home address and Social Security number. If you see anything you do not understand, call the credit reporting agency at the telephone number on the report.

[1] Kroll's activation website is only compatible with the current version or one version earlier of Chrome, Firefox, Safari and Edge. To activate services, a U.S. Social Security number and U.S. residential address is required.

Notify Law Enforcement of Suspicious Activity

You should promptly report any fraudulent activity or any suspected incidence of identity theft to proper law enforcement authorities, including local law enforcement, your state attorney general, and the Federal Trade Commission (FTC). To file a complaint with the FTC, use the below contact information or website.

The Federal Trade Commission
600 Pennsylvania Avenue, NW
Washington, DC 20580
1-877-ID-THEFT (1-877-438-4338)
TTY: 1-866-653-4261
www.IdentityTheft.gov

Complaints filed with the FTC will be added to the FTC's Identity Theft Data Clearinghouse, which is a database made available to law enforcement agencies. If you detect any suspicious activity on an account, you should promptly notify the financial institution or company which the account is maintained.

Credit Freezes

You have the right to put a security freeze, also known as a credit freeze, on your credit file, so that no new credit can be opened in your name without the use of a Personal Identification Number (PIN) that is issued when you initiate a freeze. A credit freeze is designed to prevent potential creditors from accessing your credit report without your consent. If you place a credit freeze, potential creditors and other third parties will not be able to access your credit report unless you temporarily lift the freeze. Therefore, using a credit freeze may delay your ability to obtain credit. Pursuant to federal law, you cannot be charged to place or lift a credit freeze on your credit report. Should you wish to place a credit freeze, please contact **all three** major consumer reporting agencies listed below.

Equifax	**Experian**	**TransUnion**
P.O. Box 105788	P.O. Box 9554	P.O. Box 2000
Atlanta, GA 30348-5788	Allen, TX 75013-9554	Chester, PA 19016-2000
1-800-685-1111	1-888-397-3742	1-800-916-8800
www.equifax.com/personal/credit-report-services	www.experian.com/freeze/center.html	www.transunion.com/credit-freeze

You must separately place a credit freeze on your credit file at each credit reporting agency. The following information should be included when requesting a credit freeze:

1. Your full name, with middle initial and any suffixes;
2. Your Social Security number;
3. Your date of birth (month, day, and year);
4. Your current address and previous addresses for the past five (5) years;
5. A copy of your state-issued identification card (such as a state driver's license or military ID);
6. Proof of your current residential address (such as a current utility bill or account statement); and
7. Other personal information as required by the applicable credit reporting agency.

If you request a credit freeze online or by phone, then the credit reporting agencies have one (1) business day after receiving your request to place a credit freeze on your credit file report. If you request a lift of the credit freeze online or by phone, then the credit reporting agency must lift the freeze within one (1) hour. If you request a credit freeze or lift of a credit freeze by mail, then the credit agency must place or lift the credit freeze no later than three (3) business days after getting your request. More information regarding credit freezes can be obtained from the FTC and the major consumer reporting agencies.

Fraud Alerts

You also have the right to place an initial or extended fraud alert on your file at no cost. An initial fraud alert will stay on your credit file one (1) year. The alert informs creditors of possible fraudulent activity within your report and requires the creditor to verify your 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 7 years. Should you wish to place a fraud alert, please contact any one of the three major consumer reporting agencies listed above. The agency you contact will then contact the other two. More information regarding fraud alerts can be obtained from the FTC and the major consumer reporting agencies.

Monitor Your Personal Health Information

If applicable to your situation, 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 the 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 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 records.

Additional Resources and Information

You can obtain additional information and further educate yourself regarding identity theft and the steps you can take to protect yourself by contacting your state attorney general or the FTC. The FTC's contact information and website for additional information is:

The Federal Trade Commission
600 Pennsylvania Avenue, NW
Washington, DC 20580
1-877-ID-THEFT (1-877-438-4338)
TTY: 1-866-653-4261
www.ftc.gov/idtheft

For Connecticut residents: You may contact the Connecticut Office of the Attorney General at 165 Capitol Avenue, Hartford, CT 06106; 1-860-808-5318; or https://portal.ct.gov/ag.

For District of Columbia residents: You may contact the Office of the Attorney General for the District of Columbia at 400 6th Street, NW, Washington, DC 20001; 1-202-727-3400; or https://oag.dc.gov/consumer-protection/consumer-alert-online-privacy.

For Iowa residents: You may contact law enforcement or the Iowa Attorney General's Office to report suspected incidents of identity theft. The Iowa Attorney General's Office can be reached at 1305 E. Walnut Street, Des Moines, IA 50319; 1-515-281-5164; or www.iowaattorneygeneral.gov.

For Maryland residents: You may contact the Maryland Office of the Attorney General, Consumer Protection Division, 200 St. Paul Place, Baltimore, MD 21202; 410-576-6300; 1-888-743-0023 (toll free), or https://www.marylandattorneygeneral.gov/Pages/contactus.aspx.

For Massachusetts residents: You may contact the Office of the Massachusetts Attorney General at 1 Ashburton Place, Boston, MA 02108; 1-617-727-8400; or https://www.mass.gov/orgs/office-of-the-attorney-general. You have the right to obtain a police report if you are a victim of identity theft.

For New Mexico residents: You have rights under the federal Fair Credit Reporting Act ("FCRA"). These include, among others, the right to know what is in your credit 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

https://files.consumerfinance.gov/f/201504_cfpb_summary_your-rights-under-fcra.pdf or ww.ftc.gov.

For New York residents: The 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/. You may also contact the Bureau of Internet and Technology (BIT) at 28 Liberty Street, New York, NY 10005; 212-416-8433l; or https://ag.ny.gov/about/about-office/economic-justice-division#internet-technology.

For North Carolina residents: The North Carolina Attorney General's Office may be contacted at 9001 Mail Service Center, Raleigh, NC 27699-9001; 919-716-6400; or https://ncdoj.gov/contact-doj/.

For Oregon residents: We encourage you to report suspected identity theft to the Oregon Attorney General at 1162 Court Street NE, Salem, OR 97301; 1-877-877-9392; 1-503-378-4400; or www.doj.state.or.us.

For Rhode Island residents: You may contact the Rhode Island Office of the Attorney General at 150 South Main Street, Providence, RI 02903; 1-401-274-4400; or https://riag.ri.gov/. You have the right to obtain a police report if you are a victim of identity theft. No Rhode Island residents were impacted by this breach.

For Virginia residents: You may contact the Virginia Attorney General's Office at 202 North Ninth Street, Richmond, VA 23219; 1-804-786-2071; or https://www.oag.state.va.us/contact-us/contact-info.