

CIPRIANI & WERNER

A PROFESSIONAL CORPORATION

ATTORNEYS AT LAW

JOHN LOYAL
jloyal@c-wlaw.com

450 Sentry Parkway, Suite 200
Blue Bell, Pennsylvania 19422

A Mid-Atlantic Litigation Firm

JASON MICHAEL GOODWIN
jgoodwin@c-wlaw.com

Telephone: (610) 567-0700
Fax: (610) 567-0712

Visit us online at
www.C-WLAW.com

www.C-WLAW.com

July 14, 2021

Via Email (idtheft@oag.state.md.us)

Office of the Attorney General
Attn: Security Breach Notification
200 St. Paul Place
Baltimore, MD 21202

RE: Security Incident Notification

To Whom It May Concern:

I serve as counsel for the Chester Upland School District (hereinafter "District"), and provide this notification to you of a recent data security incident. By providing this notice, the District does not waive any rights or defenses under Maryland law, including the data breach notification statute.

On February 26, 2021, the District identified suspicious activity related to an employee email account. Upon discovery, the District immediately took steps to secure the relevant account and began investigating with the assistance of a third-party forensics specialist. On March 31, 2021, the investigation confirmed that eight (8) employee email accounts experienced unauthorized access between December 14, 2020 and March 12, 2021.

Upon confirmation of the access, we immediately began an extensive programmatic and manual review of the entire contents of the email accounts to determine the type of information contained in the accounts and to whom that information related. Subsequently, the District engaged a third-party vendor to perform address verification services, including a National Change of Address Search, which was completed on June 23, 2021. As a result of its investigation, the District identified ten (10) Maryland residents potentially impacted by this incident. The type of information included the individuals' names, date of birth, Social Security numbers, and/or health insurance information.

The District is notifying the affected individuals on July 15, 2021 and providing one (1) year of complimentary credit monitoring and identity protection services. Written notice is being provided in substantially the same form as the letter attached in ***Exhibit A***. The District is also reviewing its policies and procedures related to data security.

Please contact me should you have any questions.

Very truly yours,

CIPRIANI & WERNER, P.C.

By: John Loyal
John Loyal

Exhibit A



CHESTER UPLAND SCHOOL DISTRICT

Year)

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

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

I am writing to inform you of an incident experienced by the Chester Upland School District that may have involved your personal information described below. We take the privacy and security of all information very seriously. While we have no evidence of misuse of information as a result of this incident, we are providing you with information about steps you can take to protect your information, as well as offering you complimentary identity monitoring services through Kroll.

What Happened: Chester Upland School District recently identified suspicious activity related to an employee email account. Upon discovery, we immediately took steps to secure the relevant account and began investigating with the assistance of a third-party forensic specialist. Our investigation confirmed that several District email accounts experienced unauthorized access between December 14, 2020 and March 12, 2021. Upon confirmation of the access, we immediately began an extensive programmatic and manual review of the entire contents of the email accounts to determine whether the affected email accounts contained individuals' sensitive information. After a thorough investigation the District determined that the affected email inboxes contained limited personal information of individuals and worked diligently to obtain sufficient contact information to provide you with notice of the incident.

Although the forensic investigation could not rule out the possibility that an unknown third-party actor had access to an email inbox that stored this information, there is no indication that any information has been viewed or misused at this time. We are providing this notification to you out of an abundance of caution so that you may diligently monitor your personal information and resources.

What Information Was Involved: The personal information contained in the email accounts may have included your name, in combination with the following data elements: <<b2b_text_1(DataElements)>>.

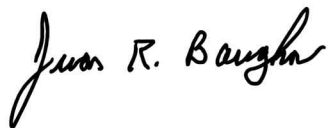
What We Are Doing: Upon learning of this incident, we immediately performed a password reset and took steps to confirm the security of our systems. Additionally, we are notifying potentially impacted individuals and offering complimentary identity monitoring services for 12 months.

What You Can Do: We encourage you to remain vigilant against incidents of identity theft and fraud by reviewing your credit reports/account statements for suspicious activity and to detect errors. If you discover any suspicious or unusual activity on your accounts, please promptly contact your financial institution or company. You may also activate the complimentary identity monitoring services we are making available to you. Due to privacy laws, we cannot register you directly. Additional information regarding how to activate the complimentary services is enclosed in the attached "Steps You Can Take to Help Protect Your Information."

For More Information: Should you have questions or concerns regarding this matter, please contact our dedicated assistance line at [1-800-828-8888](tel:1-800-828-8888) 8:00 am to 5:30 pm Central Time, Monday through Friday (excluding major US holidays).

The security of information is of the utmost importance to us, and we will continue to take steps to protect information in our care.

Sincerely,

A handwritten signature in black ink that reads "Juan R. Baughn". The signature is written in a cursive style with a large, stylized initial "J".

Juan R. Baughn, Ed. D.
Financial Recovery Receiver

STEPS YOU CAN TAKE TO HELP PROTECT YOUR INFORMATION

Activate Identity Monitoring Services

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

You have until **October 7, 2021** to activate your identity monitoring services.

Membership Number: <<Member ID_(S_N)>>

TAKE ADVANTAGE OF YOUR IDENTITY MONITORING SERVICES

You have been provided with access to the following services 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 will have the option to call a Kroll fraud specialist, who will be able to help you determine if it is 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 will be able to dig deep to uncover the scope of the identity theft, and then work to resolve it.

You can sign up for the identity monitoring service anytime between now and **October 7, 2021**. Due to privacy laws, we cannot register you directly. Activating this service will not affect your credit score.

Monitor Your Accounts

Under U.S. law, you are entitled to one free credit report annually from each of the three major credit reporting bureaus, TransUnion, Experian, and Equifax. To order your free credit report, visit www.annualcreditreport.com or call 1-877-322-8228. Once you receive your credit report, review it for discrepancies and identify any accounts you did not open or inquiries from creditors that you did not authorize. If you have questions or notice incorrect information, contact the credit reporting bureau.

You have the right to place an initial or extended “fraud alert” on a credit file at no cost. An initial fraud alert is a one-year alert that is placed on a consumer’s credit file. Upon seeing a fraud alert, 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 lasting seven years. Should you wish to place a fraud alert, please contact any of the three credit reporting bureaus listed below.

As an alternative to a fraud alert, you 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 your 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 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., III, etc.).
2. Social Security number.
3. Date of birth.
4. Address for the prior two to five years.
5. Proof of current address, such as a current utility or telephone bill.
6. A legible photocopy of a government-issued identification card (e.g., state driver’s license or identification card); 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.

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.

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

<p>TransUnion 1-800-680-7289 www.transunion.com</p> <p>TransUnion Fraud Alert P.O. Box 2000 Chester, PA 19016-2000</p> <p>TransUnion Credit Freeze P.O. Box 160 Woodlyn, PA 19094</p>	<p>Experian 1-888-397-3742 www.experian.com</p> <p>Experian Fraud Alert P.O. Box 9554 Allen, TX 75013</p> <p>Experian Credit Freeze P.O. Box 9554 Allen, TX 75013</p>	<p>Equifax 1-888-298-0045 www.equifax.com</p> <p>Equifax Fraud Alert P.O. Box 105069 Atlanta, GA 30348-5069</p> <p>Equifax Credit Freeze P.O. Box 105788 Atlanta, GA 30348-5788</p>
--	--	---

Additional Information

You can further educate yourself regarding identity theft, fraud alerts, credit freezes, and the steps you can take to protect your personal information by contacting the credit reporting bureaus, the Federal Trade Commission (FTC), or your state Attorney General. The FTC also encourages those who discover that their information has been misused to file a complaint with them. The FTC may be reached at 600 Pennsylvania Ave. NW, Washington, D.C. 20580; www.identitytheft.gov; 1-877-ID-THEFT (1-877-438-4338); and TTY: 1-866-653-4261.

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, your state Attorney General, and the FTC. This notice has not been delayed by law enforcement.

For Maryland residents, the Maryland Attorney General may be contacted at 200 St. Paul Place, 16th Floor, Baltimore, MD 21202; 1-888-743-0023; and www.oag.state.md.us. Chester Upland School District may be contacted at 232 W. 9th St., Chester, PA 19013.

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.