



MULLEN
COUGHLIN^{LLC}
ATTORNEYS AT LAW

Brittany R. Bickel
Office: (267) 930-1129
Fax: (267) 930-4771
Email: bbickel@mullen.law

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

April 24, 2024

VIA E-MAIL

Office of the Attorney General
Attn: Security Breach Notification
200 St. Paul Place
Baltimore, MD 21202
E-mail: idtheft@oag.state.md.us

Re: Notice of Data Event

To Whom It May Concern:

We represent Camino Nuevo Charter Academy (“CNCA”) located at 3435 W. Temple Street, Los Angeles, CA 90026, and are writing to notify your office of an incident that may affect the security of certain personal information relating to approximately three (3) Maryland residents. By providing this notice, CNCA does not waive any rights or defenses regarding the applicability of Maryland law, the applicability of the Maryland data event notification statute, or personal jurisdiction.

Nature of the Data Event

On July 31, 2023, CNCA became aware of suspicious activity affecting certain systems within its network, that included the encryption of certain files and systems. CNCA immediately took steps to secure its systems and launched an investigation with the assistance of third-party computer specialists to confirm the full nature and scope of the activity and to restore functionality to the affected systems. The investigation determined that an unknown actor gained access to certain CNCA systems between July 20, 2023 and July 29, 2023, and may have accessed and/or downloaded certain files stored on CNCA’s systems.

In an abundance of caution, CNCA undertook a comprehensive and time-intensive review of the involved files to determine what information was contained therein and to whom it related. Once complete, CNCA worked to confirm the identities and contact information for potentially affected individuals. CNCA’s review was recently completed and indicated that information relating to individuals was contained within files that may have been accessed by an unauthorized actor.

The information that could have been subject to unauthorized access varies by individual but includes name and Social Security number.

Notice to Maryland Residents

On or about April 24, 2024, CNCA began providing written notice of this incident to approximately three (3) Maryland residents. Written notice is being provided in substantially the same form as the letter attached here as ***Exhibit A***.

Other Steps Taken and To Be Taken

Upon becoming aware of the event, CNCA moved quickly to investigate and respond to the incident, assess the security of CNCA systems, and identify potentially affected individuals. Further, CNCA notified federal law enforcement regarding the event. CNCA is also working to implement additional safeguards and training to its employees. CNCA is providing access to credit monitoring services for one (1) year, through TransUnion, to individuals whose personal information was potentially affected by this incident, at no cost to these individuals.

Additionally, CNCA is providing impacted individuals with guidance on how to better protect against identity theft and fraud, including advising individuals to report any suspected incidents of identity theft or fraud to their credit card company and/or bank. CNCA is 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.

CNCA is also providing written notice of this incident to relevant state regulators, as necessary, and to the three major credit reporting agencies, Equifax, Experian, and TransUnion.

Contact Information

Should you have any questions regarding this notification or other aspects of the data security event, please contact us at (267) 930-4776.

Very truly yours,

Brittany R. Bickel of
MULLEN COUGHLIN LLC

BRB/jrm
Enclosure

EXHIBIT A

April 24, 2024

Notice of Data Breach

Dear _____ :

Camino Nuevo Charter Academy (“CNCA”) writes to notify you of a recent event that may have impacted some of your information. Although there is no indication that your information has been misused in relation to this event, we are providing you with information about the event, our response to it, and resources available to you to help protect your information, should you feel it appropriate to do so.

What Happened? On July 31, 2023, CNCA became aware of suspicious activity affecting certain systems within our network, that included the encryption of certain files and systems. We immediately took steps to secure our systems and launched an investigation with the assistance of third-party computer specialists to confirm the full nature and scope of the activity and to restore functionality to the affected systems. Our investigation determined that an unknown actor gained access to certain CNCA systems between July 20, 2023, and July 29, 2023, and may have accessed and/or downloaded certain files stored on our systems.

In an abundance of caution, we undertook a comprehensive and time-intensive review of the involved files to determine what information was contained therein and to whom it related. Once this process was complete, we worked to confirm the identifies and contact information for potentially affected individuals. Our review was recently completed and indicates your information was contained within files that may have been accessed by an unauthorized actor.

What Information Was Involved? The information related to you which may have been accessed includes your name and financial account information. Please note that we have no evidence of actual misuse of your personal information as a result of this event.

What We Are Doing. Safeguarding the privacy of information in our care, and the security of our network, are among our highest priorities. Upon learning of this event, we moved quickly to investigate and respond, assess the security of our systems, and notify potentially affected individuals. We also promptly notified the Federal Bureau of Investigation of this event. As part of our ongoing commitment to the security of information within our care, we are reviewing our existing policies and procedures regarding cybersecurity and evaluating additional measures and safeguards to protect against this type of event in the future. We are also implementing additional network security measures to further enhance our network security.

While we have no indication of your information being misused as a result of this event, as an added precaution, we are offering you access to Single Bureau Credit Monitoring/Single Bureau Credit Report/Single Bureau Credit Score services at no charge. These services provide you with alerts for 12 months from the date of enrollment when changes occur to your credit file. This notification is sent to you the same day that the change or update takes place with the bureau. Finally, we are providing you with proactive fraud assistance to help with any questions that you might have or in event that you become a victim of fraud. These services will be provided by Cyberscout, a TransUnion company specializing in

fraud assistance and remediation services. For enrollment instructions, please review the information contained in the attached *Steps You Can Take to Protect Your Information*.

What You Can Do. We encourage you to remain vigilant against incidents of identity theft and fraud by reviewing your account statements and monitoring your free credit reports for suspicious activity. You may also review the information contained in the attached *Steps You Can Take to Protect Your Information*. There, you will find more information on the credit monitoring and identity restoration services we are making available to you. We encourage you to activate these services as we are not able to activate them for you.

For More Information. We understand that you may have questions about this incident that are not addressed in this letter. If you have additional questions, please call our dedicated assistance line toll-free at 1-833-543-2521, Monday through Friday 8:00 a.m. – 8:00 p.m. Eastern Time, excluding U.S. holidays. You may also write to CNCA at 3435 W. Temple Street, Los Angeles, CA 90026.

Sincerely,

Adriana Abich
Chief Executive Officer

STEPS YOU CAN TAKE TO PROTECT YOUR INFORMATION

Enroll in Monitoring Services

To enroll in Credit Monitoring services at no charge, please log on to <https://bfs.cyberscout.com/activate> and follow the instructions provided. When prompted please provide the following unique code to receive services: **0FE042C67E72**. In order for you to receive the monitoring services described above, you must enroll within 90 days from the date of this letter. The enrollment requires an internet connection and e-mail account and may not be available to minors under the age of 18 years of age. Please note that when signing up for monitoring services, you may be asked to verify personal information for your own protection to confirm your identity.

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 a free credit report, visit www.annualcreditreport.com or call, toll-free, 1-877-322-8228. Consumers may also directly contact the three major credit reporting bureaus listed below to request a free copy of their 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 consumers are the victim of identity theft, they are entitled to an extended fraud alert, which is a fraud alert lasting seven years. Should consumers wish to place a fraud alert, please contact any 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 a consumer’s name without consent. However, consumers should be aware that using a credit freeze to take control over who gets access to the personal and financial information in their credit report may delay, interfere with, or prohibit the timely approval of any subsequent request or application they make regarding a new loan, credit, mortgage, or any other account involving the extension of credit. Pursuant to federal law, consumers cannot be charged to place or lift a credit freeze on their credit report. To request a credit freeze, individuals may need to provide some or all of 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 they are a victim of identity theft.

Should consumers wish to place a credit freeze or fraud alert, 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	1-800-916-8800
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

Consumers may further educate themselves regarding identity theft, fraud alerts, credit freezes, and the steps they can take to protect your personal information by contacting the consumer reporting bureaus, the Federal Trade Commission, or their state Attorney General. The Federal Trade Commission may be reached at: 600 Pennsylvania

Avenue NW, Washington, D.C. 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. Consumers can obtain further information on how to file such a complaint by way of the contact information listed above. Consumers have the right to file a police report if they ever experience identity theft or fraud. Please note that in order to file a report with law enforcement for identity theft, consumers will likely need to provide some proof that they have been a victim. Instances of known or suspected identity theft should also be reported to law enforcement and the relevant 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, D.C. 20001; (202) 442-9828; and oag.dc.gov.

For Maryland residents, the Maryland Attorney General may be contacted at: 200 St. Paul Place, 16th Floor, Baltimore, MD 21202; 1-410-576-6300 or 1-888-743-0023; and <https://www.marylandattorneygeneral.gov/>.

For New Mexico residents, consumers have rights pursuant to the Fair Credit Reporting Act, such as the right to be told if information in their credit file has been used against them, the right to know what is in their credit file, the right to ask for their 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 consumers' files is limited; consumers must give consent for credit reports to be provided to employers; consumers may limit "prescreened" offers of credit and insurance based on information in their credit report; and consumers may seek damages from violators. Consumers 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 consumers to review their 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.