Gregory J. Bautista
Office: (267) 930-1509
Fax: (267) 930-4771
Email: gbautista@mullen.law

1127 High Ridge Road, #301
Stamford, CT 06905

August 14, 2020

VIA E-MAIL

Office of the Attorney General of Iowa
Consumer Protection Division
Security Breach Notification
1305 E. Walnut Street
Des Moines, Iowa 50319-0106
E-mail: consumer@ag.iowa.gov

Re: Notice of Data Event

Dear Sir or Madam:

We represent Metropolitan Community College of Kansas City ("MCCKC"), located at 3200 Broadway Blvd., Kansas City, MO 64111, and are writing to notify your office of an incident that may affect the security of some personal information relating to one thousand and forty-nine (1049) Iowa residents. The investigation into this matter is ongoing, and this notice will be supplemented with any new significant facts learned subsequent to its submission. By providing this notice, MCCKC does not waive any rights or defenses regarding the applicability of Iowa law, the applicability of the Iowa data event notification statute, or personal jurisdiction.

Nature of the Data Event

On June 19, 2020, MCCKC determined that student and employee information may have been available to an unauthorized party due to a ransomware attack that resulted in certain data being encrypted. Following the incident, MCCKC immediately engaged a third party to conduct a forensic investigation with the objective of identifying the potential scope of access the threat actor may have had to the environment during the period of unauthorized access, which included arriving at a determination as to whether sensitive personal data was accessed by an unauthorized third party. The forensic investigation was recently completed and determined that an unauthorized individual may have had access to the MCCKC environment.

The forensic investigation did not conclude or preclude that data was extracted from MCCKC's systems however, it is possible that certain personal data, including names, Social Security numbers, drivers'

license information and medical information of former, prospective, and current students could have been accessed by an unauthorized party. The investigation further determined that the names, Social Security numbers and bank account information of employees could have been accessible as well, however, there is no evidence that any personal information was extracted from MCCKC's systems or subject to actual or attempted misuse. Although the investigation did not find any specific access to any individual's information and MCCKC has no indication that data has been extracted from MCCKC's systems or misused, MCCKC has chosen to notify all potentially impacted parties of this incident out of an abundance of caution.

Notice to Iowa Residents

On or about August 14, 2020, MCCKC provided written notice of this incident to all affected individuals, which includes one thousand and forty-nine (1049) Iowa residents. Written notice is being provided in substantially the same form as the email attached here as ***Exhibit A***.

Other Steps Taken and To Be Taken

Following confirmation that an unauthorized individual did gain access to the MCCKC network, MCCKC immediately sought to identify the population of potentially impacted individuals. MCCKC is also working to implement additional safeguards meant to further secure data within its environment. MCCKC is providing access to credit monitoring services for up to two years through *my*TrueIdentity to individuals whose personal information was potentially affected by this incident, at no cost to these individuals.

Additionally, MCCKC 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. MCCKC is providing individuals with information on how to place a fraud alert and security freeze on one's credit file, information on protecting against tax fraud, 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.

Contact Information

Should you have any questions regarding this notification or other aspects of the data security event, please contact us at (267) 930-1509.

Very truly yours,

Gregory J. Bautista of
MULLEN COUGHLIN LLC

GJB /eeb
Enclosure

EXHIBIT A

From: MCC Informational <mccinfosec@mcckc.edu>
Sent: Friday, August 14, 2020 12:00 PM
To: DL-Data Breach Team
Subject: Potential Information Security Incident

NOTICE OF DATA BREACH

Dear [redacted],

Metropolitan Community College of Kansas City ("MCCKC") takes seriously the privacy and security of its students and employees, and therefore wanted to timely release information regarding a data privacy incident involving name, Social Security number, drivers' license number, medical information and bank account information. Although we are not aware of any misuse of individual information, it is important to us that we provide information regarding this matter.

What happened?

On June 19, 2020, MCCKC determined that your information may have been available to an unauthorized party due to a ransomware attack that resulted in certain data being encrypted. Following the incident, MCCKC immediately engaged a third party to conduct a forensic investigation with the objective of identifying the potential scope of access the threat actor may have had to the environment during the period of unauthorized access, which included arriving at a determination as to whether sensitive personal data was accessed by an unauthorized third party. The forensic investigation was recently completed and determined that an unauthorized individual may have had access to the MCCKC environment. The forensic investigation did not conclude or preclude that data was extracted from MCCKC's systems however, it is possible that certain personal data, including names, Social Security numbers, drivers' license information and medical information of former, prospective, and current students could have been accessed by an unauthorized party. The investigation further acknowledged that the names, Social Security numbers and bank account information of employees could have been accessible as well, however, **there is no evidence that any personal information was extracted from MCC's systems or subject to actual or attempted misuse**. Although the investigation did not find any specific access to any individual's information and MCCKC has no indication that data has been extracted from MCCKC's systems or misused, we have chosen to notify all potentially impacted parties of this incident out of an abundance of caution and in full transparency.

What we are doing?

Following confirmation that an unauthorized individual did gain access to the MCCKC network, MCCKC immediately sought to identify the population of potentially impacted individuals. Privacy of data is a top priority for MCCKC and due to our security posture, MCCKC did not lose access to its systems, backup systems, or other operational data. However, in an abundance of caution, MCCKC has implemented additional safeguards to further secure system information.

As a precaution, we have arranged for you to enroll, at no cost to you, in an online credit monitoring service (myTrueIdentity) for one year provided by TransUnion Interactive, a subsidiary of TransUnion, ® one of the three nationwide credit reporting companies. This service includes Credit Monitoring, Fraud Consultation, and Identity Theft Restoration.

How to Enroll: You can sign up **online** or via **U.S. mail delivery**

- To enroll in this service, go to the *my*TrueIdentity website at **www.MyTrueIdentity.com** and, in the space referenced as "Enter Activation Code," enter the 12-letter Activation Code [redacted] and follow the three steps to receive your credit monitoring service online within minutes.
- If you do not have access to the Internet and wish to enroll in a similar offline, paper-based credit monitoring service, via U.S. mail delivery, please call the TransUnion Fraud Response Services toll-free hotline at 1-855-288-5422. When prompted, enter the six-digit telephone passcode [redacted] and follow the steps to enroll in the offline credit monitoring service, add an initial fraud alert to your credit file, or to speak to a TransUnion representative if you believe you may be a victim of identity theft.

You can sign up for the online or offline credit monitoring service anytime between now and **November 30, 2020**. Due to privacy laws, we cannot register you directly. Please note that credit monitoring services might not be available for individuals who do not have a credit file with TransUnion or an address in the United States (or its territories) and a valid Social Security number. Enrolling in this service will not affect your credit score.

ADDITIONAL DETAILS REGARDING YOUR 12-MONTH COMPLIMENTARY CREDIT MONITORING SERVICE:

- Once you are enrolled, you will be able to obtain one year of unlimited access to your TransUnion credit report and credit score.
- The daily credit monitoring service will notify you if there are any critical changes to your credit file at TransUnion, including fraud alerts, new inquiries, new accounts, new public records, late payments, changes of address, and more.
- The service also includes access to an identity restoration program that provides assistance in the event that your identity is compromised and up to $1,000,000 in identity theft insurance with no deductible. (Policy limitations and exclusions may apply.)

What you can do.

Please review the "Additional Resources" section included with this correspondence. This section describes additional steps you can take to help protect yourself, including recommendations by 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.

If you have questions, please call **855-907-2122** Monday through Friday from 8:00 a.m. to 8:00 p.m. Central Time. Please have your membership number ready.

Protecting your information is important to us. We trust that the services we are offering to you demonstrate our continued commitment to your security and satisfaction.

Sincerely,

John Chawana

John Chawana, Ph.D.
Vice Chancellor | Institutional Effectiveness, Research & Technology

---

Steps You Can Take to Protect Your Information

Monitor Accounts

We encourage you to remain vigilant against incidents of identity theft and fraud, to review your account statements, and to monitor your credit reports for suspicious activity. Under U.S. law you are entitled to one free credit report annually from each of the three major credit reporting bureaus. To order your free credit report, visit www.annualcreditreport.com or call, toll-free, 1-877-322-8228. You may also contact the three major credit bureaus directly to request a free copy of your credit report.

You have the right to place a "security freeze" on your credit report, which will prohibit a consumer reporting agency from releasing information in your credit report without your express authorization. The security 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 security 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 security freeze on your credit report. Should you wish to place a security freeze, please contact the major consumer reporting agencies listed below:

Experian	**TransUnion**	**Equifax**
P.O. Box 9554	P.O. Box 160	P.O. Box 105788
Allen, TX 75013	Woodlyn, PA 19094	Atlanta, GA 30348-5788
1-888-397-3742	1-888-909-8872	1-800-685-1111
www.experian.com/freeze/center.html	www.transunion.com/credit-freeze	www.equifax.com/personal/credit-report-services

In order to request a security freeze, you will need to provide the following information:

1. Your full name (including middle initial as well as Jr., Sr., II, III, etc.);
2. Social Security number;
3. Date of birth;
4. If you have moved in the past five (5) years, provide the addresses where you have lived over the prior 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, military identification, etc.);
7. If you are a victim of identity theft, include a copy of either the police report, investigative report, or complaint to a law enforcement agency concerning identity theft.

As an alternative to a security freeze, you have the right to place an initial or extended "fraud alert" on your 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 agencies listed below:

Experian	**TransUnion**	**Equifax**
P.O. Box 9554	P.O. Box 2000	P.O. Box 105069
Allen, TX 75013	Chester, PA 19016	Atlanta, GA 30348
1-888-397-3742	1-800-680-7289	1-888-766-0008
www.experian.com/fraud/center.html	www.transunion.com/fraud-victim-resource/place-fraud-alert	www.equifax.com/personal/credit-report-services

Additional Information

You can further educate yourself regarding identity theft, fraud alerts, security freezes, and the steps you can take to protect yourself by contacting the consumer reporting agencies, the Federal Trade Commission, or your state Attorney General.

The Federal Trade Commission can be reached at: 600 Pennsylvania Avenue NW, Washington, DC 20580, www.identitytheft.gov, 1-877-ID-THEFT (1-877-438-4338); 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 Maryland residents, the Attorney General can be contacted at 200 St. Paul Place, 16th Floor, Baltimore, MD 21202, 1-410-528-8662, 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 agencies must correct or delete inaccurate, incomplete, or unverifiable information; consumer reporting agencies may not report outdated negative information; access to your file is limited; you must give your consent for 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.

To unsubscribe from this list, please click on the following link: Unsubscribe