McDonald Hopkins
A business advisory and advocacy law firm®

McDonald Hopkins PLC
39533 Woodward Avenue
Suite 318
Bloomfield Hills, MI 48304
P 1.248.646.5070
F 1.248.646.5075

James J. Giszczak
Direct Dial: 248-220-1354
E-mail: jgiszczak@mcdonaldhopkins.com

October 30, 2020

VIA U.S. MAIL

Consumer Protection Division
Security Breach Notifications
Office of the Attorney General of Iowa
1305 E. Walnut Street
Des Moines, IA 50319-0106

Re: Illinois Valley Community College – Incident Notification

Dear Sir or Madam:

McDonald Hopkins PLC represents Illinois Valley Community College ("the College"). I am writing to provide notification of an incident at the College that may affect the security of personal information of approximately 602 Iowa residents. The College's investigation is ongoing, and this notification will be supplemented with any new or significant facts or findings subsequent to this submission, if any. By providing this notice, the College does not waive any rights or defenses regarding the applicability of Iowa law or personal jurisdiction.

On or about April 24, 2020, the College detected that a ransomware infection encrypted files stored on some of its servers. In addition, the College knows that data was taken by the threat actor, but it cannot be certain exactly what data was taken. Upon learning of the issue, the College contained the threat and immediately commenced a prompt and thorough investigation. As part of its investigation, the College has been working very closely with external cybersecurity professionals experienced in handling these types of incidents. The College devoted considerable time and effort to determine what information was contained in the affected servers. Based on its comprehensive investigation and document review, which concluded on September 30, 2020, the College discovered that the servers contained a limited amount of personal information, including the affected residents' names and one or more of the following: Social Security numbers, driver's license numbers, and/or financial account information.

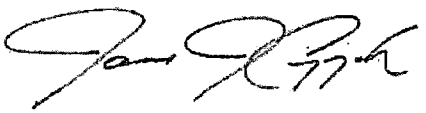
To date, the College is not aware of any reports of identity fraud or improper use of any information as a direct result of this incident. Because the College knows that data was taken, but cannot confirm that it was the affected residents' data, out of an abundance of caution, the College wanted to inform you (and the affected residents) of the incident and to explain the steps that it is taking to help safeguard the affected residents against identity fraud. The College is providing the affected residents with written notification of this incident commencing on or

about October 30, 2020 in substantially the same form as the letter attached hereto. The College is offering the affected residents whose Social Security numbers were impacted complimentary one-year memberships with a credit monitoring service. The College is advising the affected residents about the process for placing fraud alerts and/or security freezes on their credit files and obtaining free credit reports. The affected residents whose financial account information was impacted are being advised to contact their financial institutions to inquire about steps to take to protect their accounts. The affected residents are also being provided with the contact information for the consumer reporting agencies, the Federal Trade Commission, and the Iowa Attorney General.

At the College, protecting the privacy of personal information is a top priority. The College is committed to maintaining the privacy of personal information in its possession and has taken many precautions to safeguard it. The College continually evaluates and modifies its practices and internal controls to enhance the security and privacy of personal information.

Should you have any questions regarding this notification, please contact me at (248) 220-1354 or jgiszczak@mcdonaldhopkins.com. Thank you for your cooperation.

Sincerely,



James J. Giszczak

Encl.

ILLINOIS VALLEY COMMUNITY COLLEGE

[redacted]

[redacted]

Dear [redacted]:

We are writing with important information regarding a recent security incident. The privacy and security of the personal information we maintain is of the utmost importance to Illinois Valley Community College. We wanted to provide you with information about the incident, explain the services we are making available to you, and let you know that we continue to take significant measures to help protect your information.

What Happened?

On or about April 24, 2020, we detected that a ransomware infection encrypted files stored on some of our servers. In addition, we do know that data was taken by the threat actor, but we cannot be certain exactly what data was taken.

What We Are Doing.

Upon learning of the issue, we contained the threat and immediately commenced a prompt and thorough investigation. As part of our investigation, we have been working very closely with external cybersecurity professionals experienced in handling these types of incidents. We devoted considerable time and effort to determine what information was contained in the affected servers.

What Information Was Involved.

Based on our comprehensive investigation and document review, which concluded on September 30, 2020, we discovered that the servers contained your [redacted].

What You Can Do.

To date, we are not aware of any reports of identity fraud or improper use of your information as a direct result of this incident. Because we know that data was taken, but cannot confirm that it was your data, out of an abundance of caution, we wanted to make you aware of the incident, explain the services we are making available to help safeguard you against identity fraud, and suggest steps that you should take as well. To help protect you and your personal information, we have secured the services of Kroll to provide identity monitoring at no cost to you for one year. 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 personal information. Your identity monitoring services include Credit Monitoring, Fraud Consultation, and Identity Theft Restoration. Additional information describing these services, including how to activate your complimentary one-year membership, is included with this letter.

This letter also provides other precautionary measures you can take to help protect your personal information, including placing a Fraud Alert and/or Security Freeze on your credit files, and/or obtaining a free credit report. Additionally, you should always remain vigilant in reviewing your financial account statements and credit reports for fraudulent or irregular activity on a regular basis.

For More Information.

Please accept our apologies that this incident occurred. We are committed to maintaining the privacy of personal information in our possession and have taken many precautions to safeguard it. We continually evaluate and modify our practices and internal controls to enhance the security and privacy of your personal information.

If you have any further questions regarding this incident, please call our dedicated and confidential toll-free response line that we have set up to respond to questions at [redacted] Monday through Friday from 8:00 a.m. to 5:30 p.m. Central Time. This response line is staffed with professionals familiar with this incident and knowledgeable on what you can do to help protect against misuse of your information.

Sincerely,

Illinois Valley Community College

– OTHER IMPORTANT INFORMATION –

1. Activating Complimentary 12-Month Identity Monitoring.

Visit [redacted] to activate and take advantage of your identity monitoring services.

You have until ***February 1, 2021*** *to activate your identity monitoring services.*

Membership Number: [redacted]

Kroll | A Division of DUFF&PHELPS

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'll 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.

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.

2. Placing a Fraud Alert on Your Credit File.

Whether or not you choose to use the complimentary 12 month identity monitoring services, we recommend that you place an initial one-year "Fraud Alert" on your credit files, at no charge. A fraud alert tells creditors to contact you personally before they open any new accounts. To place a fraud alert, call any one of the three major credit bureaus at the numbers listed below. As soon as one credit bureau confirms your fraud alert, they will notify the others.

Equifax	**Experian**	**TransUnion LLC**
P.O. Box 105069	P.O. Box 2002	P.O. Box 2000
Atlanta, GA 30348	Allen, TX 75013	Chester, PA 19016
www.equifax.com	www.experian.com	www.transunion.com
1-800-525-6285	1-888-397-3742	1-800-680-7289

3. Consider Placing a Security Freeze on Your Credit File.

If you are very concerned about becoming a victim of fraud or identity theft, you may request a "Security Freeze" be placed on your credit file, at no charge. A security freeze prohibits, with certain specific exceptions, the consumer reporting agencies from releasing your credit report or any information from it without your express authorization. You may place a security freeze on your credit report by contacting all three nationwide credit reporting companies at the numbers below and following the stated directions or by sending a request in writing, by mail, to all three credit reporting companies:

Equifax Security Freeze	**Experian Security Freeze**	**TransUnion Security Freeze**
P.O. Box 105788	P.O. Box 9554	P.O. Box 2000
Atlanta, GA 30348	Allen, TX 75013	Chester, PA 19016
https://www.freeze.equifax.com	http://experian.com/freeze	http://www.transunion.com/securityfreeze
1-800-349-9960	1-888-397-3742	1-888-909-8872

In order to place the security freeze, you'll need to supply your name, address, date of birth, Social Security number and other personal information. After receiving your freeze request, each credit reporting company will send you a confirmation letter containing a unique PIN (personal identification number) or password. Keep the PIN or password in a safe place. You will need it if you choose to lift the freeze.

If your personal information has been used to file a false tax return, to open an account or to attempt to open an account in your name or to commit fraud or other crimes against you, you may file a police report in the City in which you currently reside.

If you do place a security freeze *prior* to enrolling in the credit monitoring service as described above, you will need to remove the freeze in order to sign up for the credit monitoring service. After you sign up for the credit monitoring service, you may refreeze your credit file.

4. Obtaining a Free Credit Report.

Under federal law, you are entitled to one free credit report every 12 months from each of the above three major nationwide credit reporting companies. Call **1-877-322-8228** or request your free credit reports online at **www.annualcreditreport.com**. Once you receive your credit reports, review them for discrepancies. Identify any accounts you did not open or inquiries from creditors that you did not authorize. Verify all information is correct. If you have questions or notice incorrect information, contact the credit reporting company.

5. Additional Helpful Resources.

Even if you do not find any suspicious activity on your initial credit reports, the Federal Trade Commission (FTC) recommends that you check your credit reports periodically. Checking your credit report periodically can help you spot problems and address them quickly.

If you find suspicious activity on your credit reports or have reason to believe your information is being misused, call your local law enforcement agency and file a police report. Be sure to obtain a copy of the police report, as many creditors will want the information it contains to absolve you of the fraudulent debts. You may also file a complaint with the FTC by contacting them on the web at www.ftc.gov/idtheft, by phone at 1-877-IDTHEFT (1-877-438-4338), or by mail at Federal Trade Commission, Consumer Response Center, 600 Pennsylvania Avenue, NW, Washington, DC 20580. Your complaint will be added to the FTC's Identity Theft Data Clearinghouse, where it will be accessible to law enforcement for their investigations. In addition, you may obtain information from the FTC about fraud alerts and security freezes.

If this notice letter states that your financial account information was impacted, we recommend that you contact your financial institution to inquire about steps to take to protect your account, including whether you should close your account or obtain a new account number.