

**Spencer S. Pollock**  
Direct Dial: 410-917-5189  
E-mail: spollock@mcdonaldhopkins.com

November 22, 2023

**VIA E-MAIL (IDTHEFT@OAG.STATE.MD.US)**

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

**Re: Bluefield University – Incident Notification**

To Whom It May Concern:

McDonald Hopkins PLC represents Bluefield University (“Bluefield”). I am writing to provide notification of an incident at Bluefield that may affect the security of personal information of three hundred and sixty-six (366) Maryland residents. Bluefield’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, Bluefield does not waive any rights or defenses regarding the applicability of Maryland law or personal jurisdiction.

On May 1, 2023, Bluefield detected unauthorized access to its network as a result of a cybersecurity incident. Bluefield immediately secured its network and commenced a prompt and thorough investigation in consultation with outside cybersecurity professionals who regularly investigate and analyze these types of situations. Bluefield devoted considerable time and effort to determine what information may have been impacted. Based on its comprehensive investigation and review, Bluefield discovered on October 26, 2023, that a limited amount of personal information was removed from its network in connection with this incident, including the affected residents’ full names and one (1) or more of the following: Social Security number, bank and/or financial account information, driver’s license number or government identification number, and health insurance information. On November 21, 2023, Bluefield located the most recent addresses of the impacted individuals.

To date, Bluefield is not aware of any reports of identity fraud or improper use of any information as a direct result of this incident. Nevertheless, out of an abundance of caution, Bluefield 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. Bluefield is providing the affected residents with written notification of this incident commencing on or about November 27, 2023 in substantially the same form as the letter attached hereto. Bluefield is offering the

affected residents whose Social Security numbers were impacted complimentary one-year memberships with a credit monitoring service. Bluefield 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 are also being provided with the contact information for the consumer reporting agencies and the Federal Trade Commission.

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

Should you have any questions concerning this notification, please contact me at (410) 917-5189 or [spollock@mcdonaldhopkins.com](mailto:spollock@mcdonaldhopkins.com). Thank you for your cooperation.

Very truly yours,

A handwritten signature in blue ink, appearing to read "Spencer S. Pollock". The signature is fluid and cursive, with the first name "Spencer" being more prominent than the last name "Pollock".

Spencer S. Pollock

Encl.



November 27, 2023

### IMPORTANT INFORMATION PLEASE

Dear [REDACTED]

The privacy and security of the personal information we maintain is of the utmost importance to Bluefield University ("Bluefield"). We are writing with important information regarding a security incident that may have involved your personal information. We want 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 protect your information.

#### What Happened?

On May 1, 2023, Bluefield detected unauthorized access to our network as a result of a cybersecurity incident that resulted in the potential exposure of the data we maintain.

#### What We Are Doing.

Upon learning of this issue, Bluefield secured its network and commenced a prompt and thorough investigation in consultation with outside cybersecurity professionals who regularly investigate and analyze these types of situations. Bluefield devoted considerable time and effort to determine what information was contained in the compromised files. Based on its comprehensive investigation and review, Bluefield discovered on October 26, 2023, that your personal information was potentially removed from our network by the unauthorized party.

#### What Information Was Involved?

The impacted files contained some of your personal information. This included your [REDACTED]

#### What You Can Do.

**We have no evidence that any of your information has been used for identity theft or financial fraud as a result of this incident.** Nevertheless, in response to the incident, we are providing you with 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 through Identity Force, a TransUnion company specializing in fraud assistance and remediation services. To enroll in this service, please refer to the instructions provided in the "Other Important Information" section provided in this letter. This letter also provides other precautionary measures you can take to protect your personal information, including placing a fraud alert and security freeze on your credit files, and 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 maintain 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.

Representatives are available for 90 days from the date of this letter, to assist you with questions regarding this incident, between the hours of [REDACTED], Monday through Friday, excluding holidays. Please call the help line at [REDACTED] and supply the fraud specialist with your unique code listed below.

Sincerely,

Ruth Blankenship  
Bluefield University  
3000 College Drive  
Bluefield, VA 24605  
(800) 872-0175

**– OTHER IMPORTANT INFORMATION –**

**1. Enrolling in Complimentary 12-Month Credit Monitoring.**

To enroll in Credit Monitoring services at no charge, please log on to [REDACTED] and follow the instructions provided. When prompted please provide the following unique code to receive services: [REDACTED]

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.



**2. Placing a Fraud Alert on Your Credit File.**

Whether or not you choose to use the complimentary 12-month credit 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***

P.O. Box 105069  
Atlanta, GA 30348-5069  
<https://www.equifax.com/personal/credit-report-services/credit-fraud-alerts/>  
(800) 525-6285

***Experian***

P.O. Box 9554  
Allen, TX 75013  
<https://www.experian.com/fraud/center.html>  
(888) 397-3742

***TransUnion***

Fraud Victim Assistance  
Department  
P.O. Box 2000  
Chester, PA 19016-2000  
<https://www.transunion.com/fraud-alerts>  
(800) 680-7289

**3. 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***

P.O. Box 105788  
Atlanta, GA 30348-5788  
<https://www.equifax.com/personal/credit-report-services/credit-freeze/>  
(888) 298-0045

***Experian Security Freeze***

P.O. Box 9554  
Allen, TX 75013  
<http://experian.com/freeze>  
(888) 397-3742

***TransUnion Security Freeze***

P.O. Box 160  
Woodlyn, PA 19094  
<https://www.transunion.com/credit-freeze>  
(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 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.

00001020280000

P

#### **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](http://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](http://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 and/or credit or debit card 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.

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.

**Maryland Residents:** You may obtain information about avoiding identity theft from the Maryland Attorney General's Office: Office of the Attorney General of Maryland, Consumer Protection Division, 200 St. Paul Place, Baltimore, MD 21202, <https://www.marylandattorneygeneral.gov/>, Telephone: 888-743-0023.

**Spencer S. Pollock**  
Direct Dial: 410-917-5189  
E-mail: [spollock@mcdonalddhopkins.com](mailto:spollock@mcdonalddhopkins.com)

January 31, 2024

**VIA E-MAIL (IDTHEFT@OAG.STATE.MD.US)**

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

**Re: Bluefield University – Supplemental Incident Notification**

To Whom It May Concern:

McDonald Hopkins PLC represents Bluefield University (“Bluefield”). **This notice serves as a supplemental notice to the November 22, 2023 notice previously submitted to your office.** Please note the underlying facts remain the same as outlined in the letter submitted previously.

Further, after additional review and research, Bluefield was able to locate the contact information for eleven (11) additional Maryland resident. As such, the total number of Maryland residents impacted is three hundred and seventy-seven (377). By providing this notice, Bluefield does not waive any rights or defenses regarding the applicability of Maryland law or personal jurisdiction.

Should you have any questions concerning this notification, please contact me at (410) 917-5189 or [spollock@mcdonalddhopkins.com](mailto:spollock@mcdonalddhopkins.com). Thank you for your cooperation.

Very truly yours,



Spencer S. Pollock

Encl.

January 31, 2024

**IMPORTANT INFORMATION PLEASE REVIEW CAREFULLY**

Dear [REDACTED]:

The privacy and security of the personal information we maintain is of the utmost importance to Bluefield University ("Bluefield"). We are writing with important information regarding a security incident that may have involved your personal information. We want 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 protect your information.

*What Happened?*

On May 1, 2023, Bluefield detected unauthorized access to our network as a result of a cybersecurity incident that resulted in the potential exposure of the data we maintain.

*What We Are Doing.*

Upon learning of this issue, Bluefield secured its network and commenced a prompt and thorough investigation in consultation with outside cybersecurity professionals who regularly investigate and analyze these types of situations. Bluefield devoted considerable time and effort to determine what information was contained in the compromised files. Based on its comprehensive investigation and review, Bluefield discovered on October 26, 2023, that your personal information was potentially removed from our network by the unauthorized party.

*What Information Was Involved?*

The impacted files contained some of your personal information. This included [REDACTED]  
[REDACTED]

*What You Can Do.*

**We have no evidence that any of your information has been used for identity theft or financial fraud as a result of this incident.** Nevertheless, in response to the incident, we are providing you with 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 twelve (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 through Identity Force, a TransUnion company specializing in fraud assistance and remediation services. To enroll in this service, please refer to the instructions provided in the "Other Important Information" section provided in this letter. This letter also provides other precautionary measures you can take to protect your personal information, including placing a fraud alert and security freeze on your credit files, and 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 maintain 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.

Representatives are available for 90 days from the date of this letter, to assist you with questions regarding this incident, between the hours of [REDACTED]  
[REDACTED] Please call the help line at [REDACTED] and supply the fraud specialist with your unique code listed below.

Sincerely,  
Ruth Blankenship  
Bluefield University  
3000 College Drive  
Bluefield, VA 24605  
(800) 872-0175

**– OTHER IMPORTANT INFORMATION –**

**1. Enrolling in Complimentary 12-Month Credit Monitoring.**

To enroll in Credit Monitoring services at no charge, please log on to [REDACTED] and follow the instructions provided. When prompted please provide the following unique code to receive services: [REDACTED]

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.

**2. Placing a Fraud Alert on Your Credit File.**

Whether or not you choose to use the complimentary 12-month credit 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***

P.O. Box 105069  
Atlanta, GA 30348-5069  
<https://www.equifax.com/personal/credit-report-services/credit-fraud-alerts/>  
(800) 525-6285

***Experian***

P.O. Box 9554  
Allen, TX 75013  
<https://www.experian.com/fraud/center.html>  
(888) 397-3742

***TransUnion***

Fraud Victim Assistance  
Department  
P.O. Box 2000  
Chester, PA 19016-2000  
<https://www.transunion.com/fraud-alerts>  
(800) 680-7289

**3. 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***

P.O. Box 105788  
Atlanta, GA 30348-5788  
<https://www.equifax.com/personal/credit-report-services/credit-freeze/>  
(888) 298-0045

***Experian Security Freeze***

P.O. Box 9554  
Allen, TX 75013  
<http://experian.com/freeze>  
(888) 397-3742

***TransUnion Security Freeze***

P.O. Box 160  
Woodlyn, PA 19094  
<https://www.transunion.com/credit-freeze>  
(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 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](http://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](http://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 and/or credit or debit card 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.

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.

**Maryland Residents:** You may obtain information about avoiding identity theft from the Maryland Attorney General's Office: Office of the Attorney General of Maryland, Consumer Protection Division, 200 St. Paul Place, Baltimore, MD 21202, <https://www.marylandattorneygeneral.gov/>, Telephone: 888-743-0023.