Buchanan
Ingersoll·Rooney

Jason R. McLean
412 562 1474
jason.mclean@bipc.com

Union Trust Building
501 Grant Street, Suite 200
Pittsburgh, PA 15219-4413
T 412 562 8800
F 412 562 1041

November 5, 2021

Consumer Protection Bureau
Office of the New Hampshire Attorney General
33 Capitol Street
Concord, NH 03301

Re: Notice of Data Security Incident

Dear Sir or Madam:

On behalf of the University of Maryland Global Campus ("UMGC"), located at 3501 University Boulevard East, Adelphi, MD 20783. I am writing to notify your Office of an incident that may affect the security of sixteen (16) New Hampshire residents. UMGC's investigation is ongoing, and this notice may be supplemented with any new significant facts learned subsequent to its submission. By providing this notice, UMGC does not waive any rights or defenses regarding the applicability of New Hampshire law or the applicability of the New Hampshire data breach notification statute.

Nature of the Data Incident

On October 7, the University of Maryland Global Campus became aware of a malware incident that targeted a UMGC server. We took the serve offline and initiated an investigation. Our preliminary investigation could not rule out the possibility of unauthorized access to files that contained personally identifiable information, including names, U.S. Social Security numbers, mailing addresses, and e-mail addresses. Out of an abundance of caution, we proactively notified sixteen (16) New Hampshire residents prior to completing the forensic investigation. However, further forensic investigation by a cybersecurity firm found no evidence the unauthorized access reached any individual data folders. We have yet to find proof that any data was exfiltrated from our system.

Because notice was sent to affected residents of your state, we are providing this notification as well. By providing this notice, UMGC does not waive any rights or defenses regarding the applicability of New Hampshire law or the applicability of the New Hampshire data breach notification statute.

Notice to New Hampshire Residents

On October 22, 2021, UMGC provided written notice of this incident to affected individuals, which includes approximately sixteen (16) New Hampshire 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

UMGC has implemented an incident response plan that includes conducting a full investigation with the assistance of external partners, notifying students, and implementing additional safeguards for university systems. In addition, UMGC has notified the proper authorities—including the FBI, the U.S. Department of Education, and the University System of Maryland. Those impacted by this incident have been offered 24 months of identity theft protection, identity theft insurance, credit monitoring, and related services free of charge through IDX, a leading provider of personal privacy and identity protection services.

Additionally, UMGC is providing impacted individuals with guidance on how to better protect against identity theft and fraud, to include information on how to place a fraud alert and security freeze on one's credit file, information on protecting against 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

UMGC prioritizes security and deeply regrets this incident. The safeguards UMGC has in place have significantly limited its impact. UMGC continues to take steps to further strengthen security protocols. Should you have any questions regarding this notification or other aspects of the data security incident, please contact me.

Sincerely,

Jason R. McLean
Counsel to University of Maryland Global Campus

UNIVERSITY OF MARYLAND
GLOBAL CAMPUS

To Enroll, Please Call:
[TFN]
Or Visit:
https://response.idx.us/umgc
Enrollment Code: [XXXXXXXX]

<<Return Address>>
<<City>>, <<State>> <<Zip>>

<<First Name>> <<Last Name>>
<<Address1>> <<Address2>>
<<City>>, <<State>> <<Zip>>

<<Date>>

Notice of Data Breach

Dear <<First Name>> <<Last Name>>,

On October 7, University of Maryland Global Campus became aware of a malware incident that targeted a UMGC server, and we subsequently launched an investigation. On October 15, as a result of that investigation, the university determined there had been unauthorized access to personally identifiable information.

This information included U.S. Social Security numbers, names, mailing addresses, and e-mail addresses. Your records were among the data that may have been accessed.

Out of concern for the security of your information, we are providing identity theft protection services free of charge through IDX, a firm with expertise in data breach and recovery services. These services include 24 months of credit and CyberScan monitoring, an insurance reimbursement policy, and fully managed identity theft recovery services. With this protection, IDX will help you resolve issues if your identity is compromised.

We encourage you to contact IDX with any questions and to enroll in the free identity protection services by calling [TFN] or visiting https://response.idx.us/umgc and using the Enrollment Code provided above. IDX representatives are available 24 hours a day, seven days a week. Please note the deadline to enroll is [Enrollment Deadline].

Please retain this letter for your records; you will need to reference the enrollment code at the top of this letter when calling or enrolling online. You will find detailed instructions for enrollment on the enclosed Recommended Steps document.

Please call [TFN] or visit https://response.idx.us/umgc for assistance or for any additional questions you may have.

Rest assured that we prioritize data security and deeply regret this incident. We continue to take steps to further strengthen the safeguards that protect your information and our systems.

Sincerely,

Martina Hansen
Senior Vice President and Chief Student Affairs Officer
University of Maryland Global Campus

(Enclosure)

Recommended Steps to help Protect your Information

1. Website and Enrollment. Go to https://response.idx.us/umgc and follow the instructions for enrollment using your Enrollment Code provided at the top of the letter.

2. Activate the credit monitoring provided as part of your IDX identity protection membership. The monitoring included in the membership must be activated to be effective. Note: You must have established credit and access to a computer and the internet to use this service. If you need assistance, IDX will be able to assist you.

3. Telephone. Contact IDX at [TFN] to gain additional information about this event and speak with knowledgeable representatives about the appropriate steps to take to protect your credit identity.

4. Review your credit reports. We recommend that you remain vigilant by reviewing account statements and monitoring credit reports. Under federal law, you also are entitled every 12 months to one free copy of your credit report from each of the three major credit reporting companies. To obtain a free annual credit report, go to www.annualcreditreport.com or call 1-877-322-8228. You may wish to stagger your requests so that you receive a free report by one of the three credit bureaus every four months.

If you discover any suspicious items and have enrolled in IDX identity protection, notify them immediately by calling or by logging into the IDX website and filing a request for help.

If you file a request for help or report suspicious activity, you will be contacted by a member of our ID Care team who will help you determine the cause of the suspicious items. In the unlikely event that you fall victim to identity theft as a consequence of this incident, you will be assigned an ID Care Specialist who will work on your behalf to identify, stop and reverse the damage quickly.

You should also know that you have the right to file a police report if you ever experience identity fraud. Please note that in order to file a crime report or incident report with law enforcement for identity theft, you will likely need to provide some kind of proof that you have been a victim. A police report is often required to dispute fraudulent items. You can report suspected incidents of identity theft to local law enforcement or to the Attorney General.

5. Place Fraud Alerts with the three credit bureaus. If you choose to place a fraud alert, we recommend you do this after activating your credit monitoring. You can place a fraud alert at one of the three major credit bureaus by phone and also via Experian's or Equifax's website. A fraud alert tells creditors to follow certain procedures, including contacting you, before they open any new accounts or change your existing accounts. For that reason, placing a fraud alert can protect you, but also may delay you when you seek to obtain credit. The contact information for all three bureaus is as follows:

Credit Bureaus

Equifax Fraud Reporting
1-866-349-5191
P.O. Box 105069
Atlanta, GA 30348-5069
www.equifax.com

Experian Fraud Reporting
1-888-397-3742
P.O. Box 9554
Allen, TX 75013
www.experian.com

TransUnion Fraud Reporting
1-800-680-7289
P.O. Box 2000
Chester, PA 19022-2000
www.transunion.com

It is necessary to contact only ONE of these bureaus and use only ONE of these methods. As soon as one of the three bureaus confirms your fraud alert, the others are notified to place alerts on their records as well. You will receive confirmation letters in the mail and will then be able to order all three credit reports, free of charge, for your review. An initial fraud alert will last for one year.

Please Note: No one is allowed to place a fraud alert on your credit report except you.

6. Security Freeze. By placing a security freeze, someone who fraudulently acquires your personal identifying information will not be able to use that information to open new accounts or borrow money in your name. You will need to contact the three national credit reporting bureaus listed above to place the freeze. Keep in mind that when you place the freeze, you will not be able to borrow money, obtain instant credit, or get a new credit card until you temporarily lift or permanently remove the freeze. There is no cost to freeze or unfreeze your credit files.

7. You can obtain additional information about the steps you can take to avoid identity theft from the following agencies. The Federal Trade Commission also encourages those who discover that their information has been misused to file a complaint with them.

California Residents: Visit the California Office of Privacy Protection (www.oag.ca.gov/privacy) for additional information on protection against identity theft.

Kentucky Residents: Office of the Attorney General of Kentucky, 700 Capitol Avenue, Suite 118 Frankfort, Kentucky 40601, www.ag.ky.gov, Telephone: 1-502-696-5300.

Maryland Residents: Office of the Attorney General of Maryland, Consumer Protection Division 200 St. Paul Place Baltimore, MD 21202, www.oag.state.md.us/Consumer, Telephone: 1-888-743-0023.

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 a 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. You can 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.

New York Residents: The Attorney General may be contacted at: Office of the Attorney General, The Capitol, Albany, NY 12224-0341; 1-800-771-7755; https://ag.ny.gov/.

North Carolina Residents: Office of the Attorney General of North Carolina, 9001 Mail Service Center Raleigh, NC 27699-9001, www.ncdoj.gov, Telephone: 1-919-716-6400.

Oregon Residents: Oregon Department of Justice, 1162 Court Street NE, Salem, OR 97301-4096, www.doj.state.or.us/, Telephone: 877-877-9392

Rhode Island Residents: Office of the Attorney General, 150 South Main Street, Providence, Rhode Island 02903, www.riag.ri.gov, Telephone: 401-274-4400

All US Residents: Identity Theft Clearinghouse, Federal Trade Commission, 600 Pennsylvania Avenue, NW Washington, DC 20580, www.consumer.gov/idtheft, 1-877-IDTHEFT (438-4338), TTY: 1-866-653-4261.