NIXON PEABODY LLP
ATTORNEYS AT LAW

NIXONPEABODY.COM
@NIXONPEABODYLLP

Jenny L. Holmes
Associate
T 585-263-1494
jholmes@nixonpeabody.com

1300 Clinton Square
Rochester, NY 14604-1792
585-263-1000

August 31, 2020

Via E-Mail and U.S. Postal Service

Gordon J. MacDonald, Attorney General
33 Capitol Street
Concord, NH 03301
attorneygeneral@doj.nh.gov

To Whom It May Concern:

On behalf of the SUNY New Paltz Foundation (the "Foundation"), I am writing to notify you of a security incident involving an inadvertent disclosure of personal information that may have affected five (5) New Hampshire residents. SUNY New Paltz Foundation is located at 1 Hawk Drive, New Paltz, New York 12561.

The Foundation was recently notified by Blackbaud, Inc., the Foundation's cloud storage service, that it was the target of a ransomware attack. After discovering the attack, Blackbaud's cyber security team, along with independent forensic experts and law enforcement, successfully prevented the cybercriminal from blocking its system access and ultimately expelled the cybercriminal from the Blackbaud systems. However, Blackbaud informed the Foundation that the cybercriminal removed a copy of Blackbaud's backup file containing some personal information.

The Foundation understands that Blackbaud paid the cybercriminal's monetary demand and received confirmation that the copy it had removed had been destroyed. Blackbaud stated that based on the nature of the incident, Blackbaud's research, and third party (including law enforcement) investigation, Blackbaud has no reason to believe that any data went beyond the cybercriminal, was or will be misused, or will be disseminated or otherwise made publicly. According to Blackbaud, this attack occurred at some point beginning on February 7, 2020 and could have been there intermittently until May 20, 2020. Due to Blackbaud and law enforcement's investigation, the Foundation was not notified until July 16, 2020.

The Foundation promptly engaged outside counsel to assist in an investigation and analysis to determine what personal information may have been affected. The Foundation is in the process of reviewing the personal information it maintains on individuals and its relationship with Blackbaud.

The Foundation will send a letter to the affected individuals informing them of this incident this week. The form of the notification letter to be sent to the affected New Hampshire residents is enclosed. The Foundation is offering credit monitoring and identity theft protection services through LifeLock to the affected New Hampshire residents for a period of one (1) year.

If you should have any additional questions or need further information regarding this incident, please do not hesitate to contact me at 585-263-1494.

Sincerely,

Jenny L. Holmes

Enclosure

New Paltz
STATE UNIVERSITY OF NEW YORK
SUNY New Paltz Foundation

NOTICE OF DATA BREACH

[DATE]

VIA E-MAIL

[ADDRESS]
[ADDRESS]
[ADDRESS]
[ADDRESS]

Dear [NAME]:

At SUNY New Paltz Foundation, we take your privacy and data security very seriously. We are writing to notify you of a security incident that may have involved some of your personal information. We are contacting you to explain the incident and provide you with steps you can take to protect yourself.

What Happened?

We were recently notified by Blackbaud, Inc., the Foundation's cloud storage service, that they were the target of a ransomware attack. After discovering the attack, Blackbaud's cyber security team, along with independent forensic experts and law enforcement, successfully prevented the cybercriminal from blocking their system access and was ultimately expelled from the Blackbaud systems. However, Blackbaud informed us that the cybercriminal removed a copy of Blackbaud's backup file containing some personal information.

We understand that Blackbaud paid the cybercriminal's monetary demand and received confirmation that the copy it had removed had been destroyed. Blackbaud stated that based on the nature of the incident, Blackbaud's research, and third party (including law enforcement) investigation, Blackbaud has no reason to believe that any data went beyond the cybercriminal, was or will be misused, or will be disseminated or otherwise made publicly.

According to Blackbaud, this attack occurred at some point beginning on February 7, 2020 and could have been there intermittently until May 20, 2020. Due to Blackbaud and law enforcement's investigation, the Foundation was not notified until July 16, 2020.

What Information Was Involved

We maintain information about you provided to us for one of the following reasons: to fund a scholarship awarded to you, to reimburse for expenses, or to pay an invoice for services provided. Therefore, the hackers may have had access to your personal information, including your name, address, e-mail, and social security number.

1 Hawk Drive • New Paltz, NY 12561-2443 • (845) 257-3240 • Fax (845) 257-4412 • www.newpaltz.edu/give

New Paltz
STATE UNIVERSITY OF NEW YORK
SUNY New Paltz Foundation

What We Are Doing

We are notifying you so that you can take immediate action to protect yourself. Ensuring the safety of your data is of the utmost importance to us. Upon learning of this incident, we worked with legal counsel to carefully investigate the data breach and Blackbaud's response and remediation efforts to ensure they met the Foundation's standards. We have been assured that Blackbaud has already implemented several changes that will protect your data from any subsequent incidents.

First, Blackbaud confirmed through testing performed by multiple third parties that the fix used to expel the cybercriminal withstands all known attack tactics. Additionally, Blackbaud stated that it is accelerating efforts to further harden their environment through enhancements to access management, network segmentation, and deployment of additional endpoint and network-based platforms.

We will continue to review our relationship with Blackbaud and to consider whether there may be a more appropriate service provider for the Foundation.

What Can You Do?

Review Your Account Statements and Notify Law Enforcement of Suspicious Activity

While we believe there is a low risk of unauthorized use of this information, we advise you to remain vigilant by reviewing your account statements and monitoring your credit reports regularly. If you see unauthorized activity on your account statements, you should contact your financial institution or payment card issuer directly. You also should promptly report any fraudulent activity or any suspected incidence of identity theft to proper law enforcement authorities and/or the Federal Trade Commission (FTC).

Enroll in Free Credit Monitoring/Identity Theft Protection Services

In addition, we have arranged with NortonLifeLock to provide you with credit report monitoring and identity theft protection for one (1) year, at no cost to you. To take advantage of this offer, please contact the Foundation via email at foundation@newpaltz.edu or by telephone at 845-257-3240. Please know that there are deadlines for enrollment. A LifeLock Standard™ membership[1] includes:

- ✓ LifeLock Identity Alert™ System†
- ✓ 24/7 Live Member Support
- ✓ Dark Web Monitoring**
- ✓ LifeLock Privacy Monitor™
- ✓ Lost Wallet Protection
- ✓ Stolen Funds Reimbursement up to $25,000 †††

[1] If your plan includes credit reports, scores, and/or credit monitoring features ("Credit Features"), two requirements must be met to receive said features: (i) your identity must be successfully verified with Equifax; and (ii) Equifax must be able to locate your credit file and it must contain sufficient credit history information. IF EITHER OF THE FOREGOING REQUIREMENTS ARE NOT MET YOU WILL NOT RECEIVE CREDIT FEATURES FROM ANY BUREAU. If your plan also includes Credit Features from Experian and/or TransUnion, the above verification process must also be successfully completed with Experian and/or TransUnion, as applicable. If verification is successfully completed with Equifax, but not with Experian and/or TransUnion, as applicable, you will not receive Credit Features from such bureau(s) until the verification process is successfully completed and until then you will only receive Credit Features from Equifax. Any credit monitoring from Experian and TransUnion will take several days to begin after your successful plan enrollment.
No one can prevent all identity theft or cybercrime. † LifeLock does not monitor all transactions at all businesses.
** These features are not enabled upon enrollment. Member must take action to get their protection.
††† Reimbursement and Expense Compensation, each with limits of up to $25,000 for Standard. And up to $1 million for coverage for lawyers and experts if needed. Benefits under the Master Policy are issued and covered by United
4819-3228-8713.1

New Paltz
STATE UNIVERSITY OF NEW YORK
SUNY New Paltz Foundation

- ✓ Personal Expense Compensation up to $25,000 †††
- ✓ Coverage for Lawyers and Experts up to $1 million †††
- ✓ U.S.-Based Identity Restoration Team
- ✓ One-Bureau Credit Monitoring1**
- ✓ Reduced Pre-Approved Credit Card Offers
- ✓ USPS Address Change Verification

For More Information.

For further information and assistance, or to take advantage of the LifeLock Standard™ membership, please contact us by emailing foundation@newpaltz.edu or by telephone at 845-257-3240. Please, also review the attached additional information for helpful steps you can take to protect your identity.

Please let us restate that we take very seriously our responsibility to safeguard your personal information. We sincerely apologize for any worry this situation may cause you.

Sincerely,

Julia Davis
Chief Financial Officer

4819-3228-8713.1

New Paltz
STATE UNIVERSITY OF NEW YORK
SUNY New Paltz Foundation

Important Identity Theft Information:

Additional Steps You Can Take to Protect Your Identity

The following are additional steps you may wish to take to protect your identity.

Review Your Accounts and Credit Reports

Regularly review statements from your accounts and periodically obtain your credit report from one or more of the national credit reporting companies. When you receive your credit report, look it over with care. If you notice anything suspicious – accounts you did not open, inquiries from creditors that you did not initiate, personal information such as a home address or Social Security number that is not accurate – or you see anything you do not understand, call the credit reporting agency at the number listed in the report. If you find fraudulent or suspicious activity in your credit reports, you should promptly report the matter to the proper law enforcement authorities. Follow the steps recommended above for reporting fraudulent or suspicious activity to law enforcement.

You may obtain a free copy of your credit report online at www.annualcreditreport.com by calling toll free 1.877.322.8228, or by mailing an Annual Credit Report Request Form (available at www.annualcreditreport.com) to: Annual Credit Report Request Service. P.O. Box 105281, Atlanta, GA, 30348-5281. You may also purchase a copy of your credit report by contacting one or more of the three national credit reporting agencies listed below.

Equifax Credit Information Services, Inc.
P.O. Box 740241
Atlanta, GA 30374
(888) 685-1111
www.equifax.corn

Experian
P.O. Box 4500
Allen, TX 75013
(888) 397-3742
www.experian.com

TransUnion
2 Baldwin Place
P.O. Box 1000
Chester, Pennsylvania
(800) 888-4213
www.transunion.com

Consider Placing a Fraud Alert

You may wish to consider contacting the fraud department of the three major credit bureaus to request that a "fraud alert" be placed on your file. A fraud alert notifies potential lenders to verify your identification before extending credit in your name.

Equifax:	Report Fraud:	1.888.766.0008
Experian:	Report Fraud:	1.888.397.3742
TransUnion:	Report Fraud:	1.800.916.8800

1 Hawk Drive • New Paltz, NY 12561-2443 • (845) 257-3240 • Fax (845) 257-4412 • www.newpaltz.edu/give

New Paltz
STATE UNIVERSITY OF NEW YORK
SUNY New Paltz Foundation

Security Freeze for Credit Reporting Agencies

You may wish to request a security freeze on your credit reports. A security freeze prohibits a credit reporting agency from releasing any information from a consumer's credit report without written authorization. However, please be aware that placing a security freeze on your credit report may delay, interfere with, or prevent the timely approval of any requests you make for new loans, credit mortgages, employment, housing or other services. If you have been a victim of identity theft, and you provide the credit reporting agency with a valid police report, it cannot charge you to place, lift or remove a security freeze. In all other cases, a credit reporting agency may charge you up to $10.00, each to place, temporarily lift, or permanently remove a security freeze.

To place a security freeze on your credit report, you must send a written request to each of the three major consumer reporting agencies by regular, certified or overnight mail at the following addresses:

- Equifax Security Freeze, P.O. Box 105788, Atlanta, GA 30348
- Experian Security Freeze, P.O. Box 9554, Allen, TX 75013
- TransUnion Security Freeze, Fraud Victim Assistance Department, 2 Baldwin Place, P.O. Box 1000, Chester, PA 19016

To request a security freeze, you will need to provide the following:

- Your full name (including middle initial, Jr., Sr., Roman numerals, etc.),
- Social Security number
- Date of birth
- Address(es) where you have lived over the prior five years
- Proof of current address such as a current utility bill
- A photocopy of a government-issued ID card
- 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
- If you are not a victim of identity theft, include payment by check, money order, or credit card (Visa, MasterCard, American Express or Discover only). Don't send cash through the mail.

The credit reporting agencies have three business days after receiving your request to place a security freeze on your credit report. The credit bureaus must also send written confirmation to you within five business days and provide you with a unique personal identification number (PIN) or password, or both that can be used by you to authorize the removal or lifting of the security freeze.

To lift the freeze to allow a specific entity or individual access to your credit report, you must call or send a written request to the credit reporting agencies by mail and include (1) proper identification (name, address, and Social Security number), (2) the PIN number or password provided to you when you placed the security freeze; and (3) the identities of those entities or individuals you would like to receive your credit report or the specific period of time you want the credit report available. The credit reporting agencies have three business days after receiving your request to lift the security freeze for those identified entities or for the specified period of time.

1 Hawk Drive • New Paltz, NY 12561-2443 • (845) 257-3240 • Fax (845) 257-4412 • www.newpaltz.edu/give

To remove the security freeze all together, you must send a written request to each of the three credit bureaus by mail and include proper identification (name, address, and Social Security number) and the PIN number or password provided to you when you placed the security freeze. The credit bureaus have three business days after receiving your request to remove the security freeze.

You have rights under the federal Fair Credit Reporting Act (FCRA). These include, among others, the right to know what is in your file; to dispute incomplete or inaccurate information; and to have consumer reporting agencies correct or delete inaccurate, incomplete, or unverifiable information. For more information about the FCRA, please visit www.consumer.ftc.gov/articles/pdf-0096-fair-credit-reporting-act.pdf or www.ftc.gov.

Suggestions If You Are a Victim of Identity Theft

- File a police report. Get a copy of the report to submit to your creditors and others that may require proof of a crime.

- Contact the U.S. Federal Trade Commission (FTC). The FTC provides useful information to identity theft victims and maintains a database of identity theft cases for use by law enforcement agencies. File a report with the FTC by calling the FTC's Identity Theft Hotline: 1.877.IDTHEFT (1.877.438.4338); online at http://www.ftc.gov/idtheft; or by mail at Identity Theft Clearinghouse, Federal Trade Commission, 600 Pennsylvania Ave., N.W., Washington, D.C. 20580. Also request a copy of the publication, "Take Charge: Fighting Back Against Identity Theft" from: http://www.ftc.gov/bcp/edu/pubs/consumer/idtheft/idt04.pdf.

- Keep a record of your contacts. Start a file with copies of your credit reports, the police reports, any correspondence, and copies of disputed bills. It is also helpful to keep a log of your conversations with creditors, law enforcement officials, and other relevant parties.

Take Steps to Avoid Identity Theft

Further information can be obtained from the FTC about steps to take to avoid identity theft through the following paths: http://www.ftc.gov/idtheft; calling 1.877.IDTHEFT (1.877.438.4338); or write to Consumer Response Center, Federal Trade Commission, 600 Pennsylvania Ave., N.W., Washington, D.C. 20580.

State-Specific Information

Iowa residents may contact law enforcement or the Iowa Attorney General's Office to report suspected incidents of identity theft. This office can be reached by visiting the website at www.iowaattorneygeneral.gov, calling (515) 281-5164 or requesting more information from the Office of the Attorney General, Hoover State Office Building, 1305 E. Walnut Street, Des Moines, IA 50319.

Maryland residents can learn more about preventing identity theft from the Maryland Office of the Attorney General, by visiting their web site at http://www.oag.state.md.us/idtheft/index.htm, calling the Identity Theft Unit at 1.410.567.6491, or requesting more information at the Identity Theft Unit, 200 St. Paul Place, 16th Floor, Baltimore, MD 21202.

1 Hawk Drive • New Paltz, NY 12561-2443 • (845) 257-3240 • Fax (845) 257-4412 • www.newpaltz.edu/give

New Paltz
STATE UNIVERSITY OF NEW YORK
SUNY New Paltz Foundation

North Carolina residents can learn more about preventing identity theft from the North Carolina Office of the Attorney General, by visiting their web site at http://www.ncdoj.gov/Help-for-Victims/ID-Theft-Victims.aspx, calling 1.919.716.6400 or requesting more information from the North Carolina Attorney General's Office, 9001 Mail Service Center Raleigh, NC 27699-9001.

Oregon residents may obtain information about preventing identity theft from the Oregon Attorney General's Office. This office can be reached by visiting the website at www.doj.state.or.us, calling (503) 378-4400 or requesting more information from the Oregon Department of Justice, 1162 Court Street NE, Salem, OR 97301-4096.

Rhode Island residents are reminded that you have the right to obtain a police report and request a security freeze as described above. The consumer reporting agencies may charge you a small fee to place a security freeze on your account, and may require that you provide certain personal information (such as your name, Social Security Number, date of birth and address) and proper identification (such as a copy of a government-issued ID card and a bill or statement) prior to honoring your request. There is no charge, however, to place, lift or remove a security freeze if you have been a victim of identity theft and you provide the consumer reporting agencies with a valid police report. Residents can learn more by contacting the Rhode Island Office of the Attorney General by phone at 1.410.274.4400 or by mail at 150 South Main Street, Providence, Rhode Island 02903.

Vermont residents may learn helpful information about fighting identity theft, placing a security freeze, and obtaining a free copy of your credit report on the Vermont Attorney General's website at http://www.atg.state.vt.us.

1 Hawk Drive • New Paltz, NY 12561-2443 • (845) 257-3240 • Fax (845) 257-4412 • www.newpaltz.edu/give