BakerHostetler

Baker&Hostetler LLP

312 Walnut Street
Suite 3200
Cincinnati, OH 45202-4074

T 513.929.3400
F 513.929.0303
www.bakerlaw.com

March 10, 2023

VIA E-MAIL (DOJ-CPB@DOJ.NH.GOV)

Attorney General John Formella
Office of the Attorney General
33 Capitol Street
Concord, NH 03301

Re: Incident Notification

Dear Attorney General Formella:

The New York Center for Research, Economic Advancement, Technology, Engineering and Science Corporation ("NY CREATES"), The State University of New York Polytechnic Institute ("SUNY Poly"), and The Research Foundation for The State University of New York (the "Research Foundation") are working to address a data security incident in the network at the campus on Fuller Road in Albany, New York (the "Location"),[1] [2] where all three organizations maintain a presence. The Location's network is separate and distinct from the networks of the Research Foundation's corporate office and the other SUNY campuses and is managed by individuals associated with the Location.

Unusual activity was recently discovered in the Location's network that caused certain systems to become unavailable. Actions were immediately taken to contain the incident, restore operations, and begin an investigation. A cybersecurity firm that has assisted other organizations in similar situations was engaged. Law enforcement also was notified, and information is being provided to support its investigation.

[1] NY CREATES is a New York nonprofit corporation operating exclusively for the charitable and public purposes of advancing scientific research, education, and economic development within the State of New York. SUNY Poly is a component part of the State University of New York, which is a system of public colleges and universities in the State of New York. The Research Foundation is a nonprofit educational corporation chartered to provide administrative services to SUNY.

[2] This notice does not waive the organizations' objection that New Hampshire lacks personal jurisdiction over them regarding any claims relating to this incident.

The evidence showed that there was unauthorized activity in the network between December 13, 2022, and December 14, 2022. During that time, an unauthorized party obtained files stored on file servers in the network. The investigation identified evidence showing some of the files obtained from the file servers, but because the evidence did not show which other files might have been viewed or obtained, the organizations conducted a careful review of files on the file servers. The organizations identified information in those files concerning current and former employees and, on February 6, 2023, identified certain employees whose information was or may have been contained in those files. The information included employees' names and one or more of the following data elements: Social Security number; driver's license number or state identification card number; tax identification number; passport number or other government-issued identification number; financial account number; payment card number; health information, such as workers' compensation information or disability claim information; health insurance policy number; or date of birth. The organizations determined that the files contained or may have contained such information concerning seven New Hampshire residents.

Beginning on March 10, 2023, a notification letter will be mailed to the New Hampshire residents in accordance with N.H. Rev. Stat. Ann. § 359-C:20 via United States First-Class mail. A copy of the notification letter is enclosed. The New Hampshire residents are being offered one year of access to a credit monitoring and identity theft protection solution. In addition, a dedicated, toll-free call center has been established that individuals can call to obtain more information regarding the incident.

To help prevent something like this from happening again, steps are being taken to further enhance the security of the network at the Location.

Please do not hesitate to contact me if you have any questions regarding this matter.

Sincerely,

Joseph L. Bruemmer
Partner

Return Mail Processing Center
P.O. Box 6336
Portland, OR 97228-6336

<<Mail ID>>
<<Name 1>>
<<Name 2>>
<<Address 1>>
<<Address 2>>
<<Address 3>>
<<Address 4>>
<<Address 5>>
<<City>><<State>><<Zip>>
<<Country>>

<<Date>>

Dear <<Name 1>>:

The New York Center for Research, Economic Advancement, Technology, Engineering and Science Corporation ("NY CREATES"), The State University of New York Polytechnic Institute ("SUNY Poly"), and The Research Foundation for The State University of New York (the "Research Foundation") understand the importance of protecting information. You are receiving this notice because you or a family member have a present or past affiliation with one or more of those organizations and your information may have been involved in a recent data security incident at the campus on Fuller Road in Albany, New York (the "Location"), where all three organizations have a presence. This notice explains who the organizations are, what happened, what measures were taken in response, and what you can do going forward.

Who Are We, and Why Do We Have Your Information?
NY CREATES is a New York nonprofit corporation operating exclusively for the charitable and public purposes of advancing scientific research, education, and economic development within the State of New York. SUNY Poly is a component of The State University of New York, which is a system of public colleges and universities in the State of New York. The Research Foundation is a nonprofit educational corporation chartered to provide administrative services to SUNY. One or more of these organizations have your information because you are a current or former employee, a dependent or beneficiary of a current or former employee, or a vendor of one or more of the organizations, or for another business-related reason.

What Happened?
Unusual activity was recently discovered in the network at the Location that caused certain systems to become unavailable. Actions were immediately taken to contain the incident, restore operations, and begin an investigation. A cybersecurity firm that has assisted other organizations in similar situations was engaged. Law enforcement also was notified, and information is being provided to support its investigation.

The evidence showed that there was unauthorized activity on the network between December 13, 2022, and December 14, 2022. During that time, an unauthorized party obtained files stored on file servers in the network.

What Information Was Involved?
The investigation identified evidence showing some of the files obtained from the file servers, but because the evidence did not show which other files might have been viewed or obtained, the organizations conducted a careful review of files on the file servers. The organizations identified information in those files concerning current and former employees and, between January 30, 2023 and February 6, 2023, identified certain employees whose information was or may have been contained in those files. The information included employees' names and addresses and one or more of the following data elements: Social Security number; driver's license number or state identification card number; tax identification number; passport number or other government-issued identification number; financial account number; payment card number; health information, such as workers' compensation information or disability claim information; health insurance policy number; or date of birth. You are receiving this letter because you are one of the employees whose information was or may have been contained in the files on the file servers.

What We Are Doing.
The organizations are taking this matter seriously. To help prevent something like this from happening again, steps are being taken to further enhance the security of the network at the Location.

What You Can Do.
Although the evidence did not show whether your information was viewed or obtained, you are receiving this notice so that you can take steps to protect your information. Arrangements have been made for you to receive one year of access to Equifax Complete™ Premier, a credit monitoring and identity theft protection solution. Activating this product will not hurt your credit score. For more information on identity theft prevention and Equifax Complete™ Premier, including instructions on how to activate the product, as well as some additional steps you can take in response, please review the pages that follow this letter.

For More Information
The organizations regret that this occurred and apologize for any inconvenience. If you have additional questions, please call 888-635-1206, Monday through Friday, between 9:00a m. and 9:00p m Eastern Time.

Sincerely,

NY CREATES
SUNY Poly
Research Foundation

Equifax Complete™ Premier

*Note: You must be over age 18 with a credit file to take advantage of the product

Key Features

- Annual access to your 3-bureau credit report and VantageScore[1] credit scores
- Daily access to your Equifax credit report and 1-bureau VantageScore credit score
- 3-bureau credit monitoring[2] with email notifications of key changes to your credit reports
- WebScan notifications[3] when your personal information, such as Social Security Number, credit/debit card or bank account numbers are found on fraudulent Internet trading sites
- Automatic fraud alerts[4], which encourages potential lenders to take extra steps to verify your identity before extending credit, plus blocked inquiry alerts and Equifax credit report lock[5]
- Identity Restoration to help restore your identity should you become a victim of identity theft, and a dedicated Identity Restoration Specialist to work on your behalf
- Up to $1,000,000 of identity theft insurance coverage for certain out of pocket expenses resulting from identity theft[6].
- Lost Wallet Assistance if your wallet is lost or stolen, and one-stop assistance in canceling and reissuing credit, debit and personal identification cards.

Enrollment Instructions

Go to ***www.equifax.com/activate***

Enter your unique Activation Code of <<*ACTIVATION CODE*>> then click "Submit" and follow these 4 steps:

1. **Register:**
   Complete the form with your contact information and click "Continue".
   If you already have a myEquifax account, click the 'Sign in here' link under the "Let's get started" header.
   Once you have successfully signed in, you will skip to the Checkout Page in Step 4.
2. **Create Account:**
   Enter your email address, create a password, and accept the terms of use.
3. **Verify Identity:**
   To enroll in your product, we will ask you to complete our identity verification process.
4. **Checkout**:
   Upon successful verification of your identity, you will see the Checkout Page.
   Click 'Sign Me Up' to finish enrolling.

You're done!

The confirmation page shows your completed enrollment.
Click "View My Product" to access the product features.

---

[1]*The credit scores provided are based on the VantageScore® 3.0 model. For three-bureau VantageScore credit scores, data from Equifax®, Experian®, and TransUnion® are used respectively. Any one-bureau VantageScore uses Equifax data. Third parties use many different types of credit scores and are likely to use a different type of credit score to assess your creditworthiness.*

[2]*Credit monitoring from Experian and TransUnion will take several days to begin.*

[3]*WebScan searches for your Social Security Number, up to 5 passport numbers, up to 6 bank account numbers, up to 6 credit/debit card numbers, up to 6 email addresses, and up to 10 medical ID numbers. WebScan searches thousands of Internet sites where consumers' personal information is suspected of being bought and sold, and regularly adds new sites to the list of those it searches. However, the Internet addresses of these suspected Internet trading sites are not published and frequently change, so there is no guarantee that we are able to locate and search every possible Internet site where consumers' personal information is at risk of being traded.*

[4]*The Automatic Fraud Alert feature is made available to consumers by Equifax Information Services LLC and fulfilled on its behalf by Equifax Consumer Services LLC.*

[5]*Locking your Equifax credit report will prevent access to it by certain third parties. Locking your Equifax credit report will not prevent access to your credit report at any other credit reporting agency. Entities that may still have access to your Equifax credit report include: companies like Equifax Global Consumer Solutions, which provide you with access to your credit report or credit score, or monitor your credit report as part of a subscription or similar service; companies that provide you with a copy of your credit report or credit score, upon your request; federal, state and local government agencies and courts in certain circumstances; companies using the information in connection with the underwriting of insurance, or for employment, tenant or background screening purposes; companies that have a current account or relationship with you, and collection agencies acting on behalf of those whom you owe; companies that authenticate a consumer's identity for purposes other than granting credit, or for investigating or preventing actual or potential fraud; and companies that wish to make pre-approved offers of credit or insurance to you. To opt out of such pre-approved offers, visit www.optoutprescreen.com.*

[6]*The Identity Theft Insurance benefit is underwritten and administered by American Bankers Insurance Company of Florida, an Assurant company, under group or blanket policies issued to Equifax, Inc., or its respective affiliates for the benefit of its Members. Please refer to the actual policies for terms, conditions, and exclusions of coverage. Coverage may not be available in all jurisdictions.*

ADDITIONAL STEPS YOU CAN TAKE

We remind you it is always advisable to be vigilant for incidents of fraud or identity theft by reviewing your account statements and free credit reports for any unauthorized activity. You may obtain a copy of your credit report, free of charge, once every 12 months from each of the three nationwide credit reporting companies. To order your annual free credit report, please visit www.annualcreditreport.com or call toll free at 1-877-322-8228. Contact information for the three nationwide credit reporting companies is as follows:

- *Equifax*, PO Box 740241, Atlanta, GA 30374, www.equifax.com, 1-888-378-4329
- *Experian*, PO Box 2002, Allen, TX 75013, www.experian.com, 1-888-397-3742
- *TransUnion*, PO Box 1000, Chester, PA 19016, www.transunion.com, 1-800-916-8800

If you believe you are the victim of identity theft or have reason to believe your personal information has been misused, you should immediately contact the Federal Trade Commission and/or the Attorney General's office in your state. You can obtain information from these sources about steps an individual can take to avoid identity theft as well as information about fraud alerts and security freezes. You should also contact your local law enforcement authorities and file a police report. Obtain a copy of the police report in case you are asked to provide copies to creditors to correct your records. Contact information for the Federal Trade Commission is as follows:

- *Federal Trade Commission*, Consumer Response Center, 600 Pennsylvania Avenue NW, Washington, DC 20580, 1-877-IDTHEFT (438-4338), www.ftc.gov/idtheft

Fraud Alerts and Credit or Security Freezes:

Fraud Alerts: There are two types of general fraud alerts you can place on your credit report to put your creditors on notice that you may be a victim of fraud—an initial alert and an extended alert. You may ask that an initial fraud alert be placed on your credit report if you suspect you have been, or are about to be, a victim of identity theft. An initial fraud alert stays on your credit report for one year. You may have an extended alert placed on your credit report if you have already been a victim of identity theft with the appropriate documentary proof. An extended fraud alert stays on your credit report for seven years.

To place a fraud alert on your credit reports, contact one of the nationwide credit bureaus. A fraud alert is free. The credit bureau you contact must tell the other two, and all three will place an alert on their versions of your report.

For those in the military who want to protect their credit while deployed, an Active Duty Military Fraud Alert lasts for one year and can be renewed for the length of your deployment. The credit bureaus will also take you off their marketing lists for pre-screened credit card offers for two years, unless you ask them not to.

Credit or Security Freezes: You have the right to put a credit freeze, also known as a security freeze, on your credit file, free of charge, which makes it more difficult for identity thieves to open new accounts in your name. That's because most creditors need to see your credit report before they approve a new account. If they can't see your report, they may not extend the credit.

How do I place a freeze on my credit reports? There is no fee to place or lift a security freeze. Unlike a fraud alert, you must separately place a security freeze on your credit file at each credit reporting company. For information and instructions on how to place a security freeze, contact each of the credit reporting agencies at the addresses below:

- **Experian Security Freeze**, PO Box 9554, Allen, TX 75013, www.experian.com
- **TransUnion Security Freeze**, PO Box 160, Woodlyn, PA 19094, www.transunion.com
- **Equifax Security Freeze**, PO Box 105788, Atlanta, GA 30348, www.equifax.com

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 bureau will provide you with 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.

How do I lift a freeze? A freeze remains in place until you ask the credit bureau to temporarily lift it or remove it altogether. If the request is made online or by phone, a credit bureau must lift a freeze within one hour. If the request is made by mail, then the bureau must lift the freeze no later than three business days after getting your request.

If you opt for a temporary lift because you are applying for credit or a job, and you can find out which credit bureau the business will contact for your file, you can save some time by lifting the freeze only at that particular credit bureau. Otherwise, you need to make the request with all three credit bureaus.

New York Center for Research, Economic Advancement, Technology, Engineering and Science Corporation is located at 257 Fuller Road, Albany, New York 12203 and can be reached at (518) 437-8686.

The State University of New York Polytechnic Institute is located at 257 Fuller Road, Albany, New York 12203 and can be reached at (518) 437-8686.

The Research Foundation for the State University of New York is located at 257 Fuller Road, Albany, New York 12203 and can be reached at (518) 437-8686.

Additional Information for Residents of the Following States

Maryland: You may contact and obtain information from your state attorney general at: *Maryland Attorney General's Office*, 200 St. Paul Place, Baltimore, MD 21202, 1-888-743-0023 / 1-410-576-6300, www.oag.state.md.us

New York: You may contact and obtain information from these state agencies: *New York Department of State Division of Consumer Protection*, One Commerce Plaza, 99 Washington Ave., Albany, NY 12231-0001, 518-474-8583 / 1-800-697-1220, http://www.dos.ny.gov/consumerprotection | *New York State Office of the Attorney General*, The Capitol, Albany, NY 12224-0341, 1-800-771-7755, https://ag ny.gov

North Carolina: You may contact and obtain information from your state attorney general at: *North Carolina Attorney General's Office*, 9001 Mail Service Center, Raleigh, NC 27699, 1-919-716-6000 / 1-877-566-7226, www ncdoj.gov

Rhode Island: This incident involves <<RI#>> Rhode Island residents. Under Rhode Island law, you have the right to file and obtain a copy of a police report. You also have the right to request a security freeze, as described above. You may contact and obtain information from your state attorney general at: *Rhode Island Attorney General's Office*, 150 South Main Street, Providence, RI 02903, 1-401-274-4400, www riag ri.gov

A Summary of Your Rights Under the Fair Credit Reporting Act: The federal Fair Credit Reporting Act (FCRA) promotes the accuracy, fairness, and privacy of information in the files of consumer reporting agencies. There are many types of consumer reporting agencies, including credit bureaus and specialty agencies (such as agencies that sell information about check writing histories, medical records, and rental history records). Your major rights under the FCRA are summarized below. For more information, including information about additional rights, go to www.consumerfinance.gov/learnmore or write to: Consumer Financial Protection Bureau, 1700 G Street N.W., Washington, DC 20552.

- You must be told if information in your file has been used against you.
- You have the right to know what is in your file.
- You have the right to ask for a credit score.
- You have the right to dispute incomplete or inaccurate information.
- 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 reports to be provided to employers.
- You may limit "prescreened" offers of credit and insurance you get based on information in your credit report.
- You have a 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.
- You may seek damages from violators.
- Identity theft victims and active duty military personnel have additional rights.