

RECEIVED

RECEIVED

OCT 23 2020

OCT 23 2020

CONSUMER PROTECTION CONSUMER PROTECTION

**BakerHostetler**

**Baker&Hostetler LLP**

11601 Wilshire Boulevard  
Suite 1400  
Los Angeles, CA 90025-0509

T 310.820.8800  
F 310.820.8859  
www.bakerlaw.com

M. Scott Koller  
direct dial: 310.979.8427  
mskoller@bakerlaw.com

October 22, 2020

**VIA OVERNIGHT MAIL**

Attorney General Gordon MacDonald  
Office of the Attorney General  
33 Capitol Street  
Concord, NH 03301

*Re: Incident Notification*

Dear Attorney General MacDonald:

We are writing on behalf of our client, The University of Utah (the "University"), to notify you of a ransomware attack that affected the computing servers in the University's College of Social and Behavioral Science ("CSBS").

On July 19, 2020, the University became aware that computing servers in the CSBS experienced a ransomware attack, which rendered its servers temporarily inaccessible. The University immediately took steps to secure its network, began restoring data from backups, and an external firm that specializes in responding to ransomware attacks was engaged. An investigation and analysis conducted by the University indicates that the original date of intrusion was July 16, 2020.

The University reviewed the affected data files to identify individuals whose information may have been accessed by the attackers. From this review, in August 2020, the University determined that the data files contained some personal information, including Social Security numbers, credit card information and bank account information.

Beginning on October 21, 2020, the University will mail a notification letter via United States Postal Service First-Class mail to one New Hampshire resident in accordance with N.H. Rev. Stat. Ann. § 359-C:20. A copy of the notification letter is enclosed.<sup>1</sup> The University is offering individuals whose personal information was potentially affected a complimentary one-year membership in credit monitoring and identity theft protection services from Experian®. The University has also provided a telephone number for potentially affected individuals to call with any questions they may have.

---

<sup>1</sup> This report is not, and does not constitute, a waiver of the University's objection that New Hampshire lacks personal jurisdiction over the University regarding this incident.

Atlanta Chicago Cincinnati Cleveland Columbus Costa Mesa Denver  
Houston Los Angeles New York Orlando Philadelphia Seattle Washington, DC

Office of the Attorney General

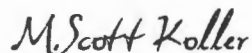
October 21, 2020

Page 2

To further protect customer information, the University has made substantial investments in technology to monitor and protect the University community against attacks, including ransomware threats. Networks and IT infrastructure are monitored 24 hours a day, and the IT environment is continuously assessed to identify any vulnerabilities that need to be addressed. The University is working to move all college systems with private and restricted data to central services to provide a more secure and protected environment. The University is also unifying the campus to one central Active Directory and moving college networks into the centrally managed University network. These steps, in addition to individuals using strong passwords and two-factor authentication, are expected to reduce the likelihood of an incident like this occurring again.

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

Sincerely,

A handwritten signature in cursive script that reads "M. Scott Koller".

Scott Koller

Enclosures



**COLLEGE OF SOCIAL  
AND BEHAVIORAL SCIENCE**

**Departments**

Anthropology  
Economics  
Family & Consumer Studies  
Geography  
Political Science  
Psychology  
Sociology

**Programs**

Criminology  
Environmental &  
Sustainability Studies  
Health, Society & Policy  
Master of Public Administration  
Master of Public Policy  
Master of Science in International  
Affairs and Global Enterprise

**ROTC**

Aerospace Studies  
Military Science  
Naval Science

**Institutes and Centers**

Archaeological Center  
Child & Family Development Center  
DIGIT Center  
National Center for Veterans Studies  
NEXUS  
Tanner Human Rights Center

[NAME]  
[ADDRESS]  
[CITY]  
[STATE] [ZIP]

October 21, 2020

**Notice of Data Breach**

Dear [NAME]:

We are writing to inform you of an incident that may have involved some of your information. This notice explains the incident, measures the University of Utah has taken, and steps you can take in response.

*What Happened?*

On Sunday, July 19, 2020, computing servers in the University of Utah's College of Social and Behavioral Science (CSBS) experienced a criminal ransomware attack, which rendered its servers temporarily inaccessible. The University immediately took steps to secure its network, began restoring data from backups, and an external firm that specializes in responding to ransomware attacks was engaged.

*What Information Was Involved?*

On August 19, 2020, our investigation determined that, during the incident, some of your personal information may have been accessed, including your [Variable Data].

*What You Can Do:*

Even though we have no evidence that your personal information has been misused, we wanted to let you know this happened and share the steps we are taking in response. As a precaution, we are offering you a complimentary membership of Experian's® IdentityWorks<sup>SM</sup>. This product provides you with identity detection and resolution of identity theft. IdentityWorks is completely free to you and enrolling in this program will not hurt your credit score. For more information on IdentityWorks, including instructions on how to activate your complimentary one-year membership, as well as some additional steps you can take in response, please see the additional information provided in the following pages.

*What We Are Doing:*

The University has made substantial investments in technology to monitor and protect the University community against attacks, including ransomware threats. Networks and IT infrastructure are monitored 24 hours a day, and the IT environment is continuously assessed to identify any vulnerabilities that need to be addressed. The University is working to move all college systems with private and restricted data to central services to provide a more secure and protected

**Office of the Dean**  
Gardner Commons Suite 3725  
260 South Central Campus Drive  
Salt Lake City, Utah 84112

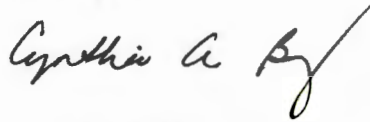
*Inspiring human solutions to life's challenges*

environment. The University is also unifying the campus to one central Active Directory and moving college networks into the centrally managed University network. These steps, in addition to individuals using strong passwords and two-factor authentication, are expected to reduce the likelihood of an incident like this occurring again.

*For More Information*

We regret that this occurred and apologize for any inconvenience. Should you have any further questions or concerns regarding this matter, please do not hesitate to contact us at 1-801-581-1887.

Sincerely,

A handwritten signature in black ink that reads "Cynthia A. Berg". The signature is written in a cursive style with a large, sweeping initial "C".

Cynthia A. Berg  
Dean and Distinguished Professor of Psychology

### Activate IdentityWorks Credit 3B Now in Three Easy Steps

To help protect your identity, we are offering a **complimentary** one-year membership of Experian IdentityWorks<sup>SM</sup> Credit 3B. This product helps detect possible misuse of your personal information and provides you with superior identity protection support focused on immediate identification and resolution of identity theft.

1. ENROLL by: **12.31.20** (Your code will not work after this date.)
2. VISIT the **Experian IdentityWorks website** to enroll:  
<https://www.experianidworks.com/3bcredit>
3. PROVIDE the **Activation Code: [Code]**

If you have questions about the product, need assistance with identity restoration or would like an alternative to enrolling in Experian IdentityWorks online, please contact Experian's customer care team at **877-288-8057**. Be prepared to provide engagement number [REDACTED] as proof of eligibility for the identity restoration services by Experian.

#### ADDITIONAL DETAILS REGARDING YOUR 12-MONTH EXPERIAN IDENTITYWORKS CREDIT 3B MEMBERSHIP:

A credit card is **not** required for enrollment in Experian IdentityWorks Credit 3B.

You can contact Experian **immediately without needing to enroll in the product** regarding any fraud issues. Identity Restoration specialists are available to help you address credit and non-credit related fraud. Once you enroll in Experian IdentityWorks, you will have access to the following additional features:

- **Experian credit report at signup:** See what information is associated with your credit file. Daily credit reports are available for online members only.\*
- **Credit Monitoring:** Actively monitors Experian, Equifax and Transunion files for indicators of fraud.
- **Experian IdentityWorks ExtendCARE™:** You receive the same high-level of Identity Restoration support even after your Experian IdentityWorks membership has expired.
- **\$1 Million Identity Theft Insurance\*\*:** Provides coverage for certain costs and unauthorized electronic fund transfers.

Activate your membership today at <https://www.experianidworks.com/3bcredit>  
or call **877-288-8057** to register with the activation code above.

**What you can do to protect your information:** There are additional actions you can consider taking to reduce the chances of identity theft or fraud on your account(s). Please refer to [www.ExperianIDWorks.com/restoration](http://www.ExperianIDWorks.com/restoration) for this information. If you have any questions about IdentityWorks, need help understanding something on your credit report or suspect that an item on your credit report may be fraudulent, please contact Experian's customer care team at **877-288-8057**.

\* Offline members will be eligible to call for additional reports quarterly after enrolling.

\*\* The Identity Theft Insurance is underwritten and administered by American Bankers Insurance Company of Florida, an Assurant company. 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](http://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](http://www.equifax.com), 1-800-685-1111
- *Experian*, PO Box 2002, Allen, TX 75013, [www.experian.com](http://www.experian.com), 1-888-397-3742
- *TransUnion*, PO Box 2000, Chester, PA 19016, [www.transunion.com](http://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](http://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 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](http://www.experian.com)
- **TransUnion Security Freeze**, PO Box 2000, Chester, PA 19016, [www.transunion.com](http://www.transunion.com)
- **Equifax Security Freeze**, PO Box 105788, Atlanta, GA 30348, [www.equifax.com](http://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.

### **Additional information for residents of 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>; and *New York State Office of the Attorney General*, The Capitol, Albany, NY 12224-0341, 1-800-771-7755, <https://ag.ny.gov>