BakerHostetler

Baker&Hostetler LLP

312 Walnut Street
Suite 3200
Cincinnati, OH 45202-4074

T 513.929.3400
F 513.929.0303
www.bakerlaw.com

Joseph L. Bruemmer
direct dial: 513.929.3410
jbruemmer@bakerlaw.com

August 4, 2021

**VIA E-MAIL (DOJ-CPN@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:

We are writing on behalf of our client, Arcadia University ("Arcadia"), to notify you of a security incident involving 24 New Hampshire residents. Arcadia University is a private university in Glenside, Pennsylvania.

On March 18, 2021 Arcadia identified a security incident that caused certain devices in the network to become unresponsive. Arcadia immediately began to investigate, a cybersecurity firm was engaged, and measures were taken to address the incident and to restore operations. Law enforcement was also notified, and Arcadia worked to support its investigation. The investigation determined that there was unauthorized activity on Arcadia's network between March 15 and March 18, 2021, and certain files on a file server were accessed. After taking measures to address the incident and restore operations, Arcadia then conducted a thorough review of the files that were accessed. Arcadia completed the review on June 7, 2021, which determined that identified files on the server contained personal information pertaining to 24 New Hampshire residents, including their names, Social Security numbers, and/or financial account information. For individuals identified by this file review, Arcadia then had to use other resources to look for a mailing address because many of the records did not contain addresses. Arcadia completed this process on July 23, 2021.

Beginning today, August 4, 2021, Arcadia University is providing written notice to the New Hampshire residents by mailing a letter via United States Postal Service First-Class mail.[1] A

[1] This report does not waive Arcadia's objection that New Hampshire lacks personal jurisdiction over it related to any claims that may arise from this incident.

sample copy of the notification letter is enclosed. Arcadia is offering a complimentary, one-year membership of credit monitoring and identity theft prevention services provided by IDX to the New Hampshire residents with Social Security numbers involved. Arcadia is also recommending that individuals remain vigilant to the possibility of fraud by reviewing their account statements for unauthorized activity. In addition, Arcadia established a dedicated phone number where the individuals may obtain more information regarding the incident.

To help prevent a similar incident from occurring in the future, Arcadia has taken additional steps to enhance existing electronic security protocols and re-educate all staff for awareness on these types of incidents.

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

Sincerely,

Joseph L. Bruemmer
Counsel

Enclosure

ARCADIA UNIVERSITY
FOUNDED 1853

P.O. Box 1907
Suwanee, GA 30024
<<Name 1>>
<<Name 2>>
<<Address 1>>
<<Address 2>>
<<Address 3>>
<<Address 4>>
<<Address 5>>
<<City>><<State>><<Zip>>
<<Country>>

To Enroll, Please Call:
1-833-909-3929
Or Visit:
https://app.idx.us/account-creation/protect
Enrollment Code: [XXXXXXXX]

August 4, 2021

Dear <<Name1>>:

At Arcadia University, we understand the importance of protecting the information we maintain. We are writing to inform you of an incident that may have involved some of your information. While we are unaware of any actual or attempted misuse of your personal information, out of an abundance of caution, we are providing you with this notice that explains the incident, measures we have taken, and some steps you may consider taking.

We identified a security incident on March 18, 2021 that caused certain devices in our network to become unresponsive. We immediately began to investigate, a cybersecurity firm was engaged, and measures were taken to address the incident and to restore operations. We also notified law enforcement and worked to support its investigation.

The investigation determined that there was unauthorized activity on our network between March 15 and March 18, 2021, and certain files on a file server were accessed. After taking measures to address the incident and restore operations, we then conducted a thorough review of the files that were accessed. The review, completed on June 7, 2021, identified files on the server that contained your <<Variable Data 1>>. For individuals identified by this file review, we then had to use other resources to look for a mailing address because many of the records did not contain addresses. We completed this process on July 23, 2021.

We wanted to notify you of this incident and to assure you that we take it seriously. As a precaution, we have arranged for you to receive a complimentary one-year membership to identity theft protection services through IDX, the data breach and recovery services expert. IDX identity protection services include 12 months of fully managed ID theft recovery services and a $1,000,000 insurance reimbursement policy. With this protection, IDX will help you resolve issues if your identity is compromised. For more information on identity theft prevention and IDX, 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 this letter.

Your confidence and trust are important to us, and we regret any inconvenience or concern this incident may cause. The confidentiality, privacy, and security of information in our care is one of our highest priorities. To further protect personal information, we have taken additional steps to enhance our existing electronic security protocols and re-educate our staff for awareness on these types of incidents. If you have any questions, please call 1-833-909-3929, Monday through Friday from 9:00 A.M. through 9:00 P.M. Eastern Time. Please note the deadline to enroll is November 4, 2021.

Sincerely,

Rashmi Radhakrishnan

Rashmi Radhakrishnan
Vice President/CIO
Arcadia University

**Recommended Steps to help Protect your Information**

**1**. **Website and Enrollment.** Go to https://app.idx.us/account-creation/protect 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 1-833-909-3929 to gain additional information about this event and speak with knowledgeable representatives about the appropriate steps to take to protect your credit identity.

If you discover any suspicious items and have enrolled in IDX identity protection, notify IDX 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.

## 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, 1-800-685-1111
- *Experian*, PO Box 2002, Allen, TX 75013, www.experian.com, 1-888-397-3742
- *TransUnion*, PO Box 2000, 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 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 2000, Chester, PA 19016, 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.

You may also contact Arcadia University at 450 S Easton Rd, Glenside, PA 19038 and (215) 572-2900.

**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; and *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 Centre, Raleigh, NC 27699, 1-919-716-6000 / 1-877-566-7226, www.ncdoj.gov .

**Rhode Island:** This incident involves <<#>> individuals in Rhode Island. 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

**West Virginia:** You have the right to ask that nationwide consumer reporting agencies place "fraud alerts" in your file to let potential creditors and others know that you may be a victim of identity theft, as described above. You also have a right to place a security freeze on your credit report, as described above.

**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). Here is a summary of your major rights under FCRA. 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.