



MULLEN  
COUGHLIN<sup>LLC</sup>  
ATTORNEYS AT LAW

RECEIVED

APR 01 2019

CONSUMER PROTECTION

Jeffrey J. Boogay  
Office: 267-930-4784  
Fax: 267-930-4771  
Email: jboogay@mullen.law

1275 Drummers Lane, Suite 302  
Wayne, PA 19087

March 26, 2019

**VIA U.S. MAIL**

Attorney General Gordon J. MacDonald  
Office of the New Hampshire Attorney General  
Attn: Security Breach Notification  
33 Capitol Street  
Concord, NH 03301

**Re: Notice of Data Security Event**

Dear Attorney General MacDonald:

We represent Arcadia University ("Arcadia") located at 450 South Easton Road, Glenside, Pennsylvania 19038. We write to notify your office of an incident that may affect the security of some personal information relating to three (3) New Hampshire residents. The investigation into this matter is ongoing, and this notice will be supplemented with any new significant facts learned subsequent to its submission. By providing this notice, Arcadia does not waive any rights or defenses regarding the applicability of New Hampshire law, the applicability of the New Hampshire data event notification statute, or personal jurisdiction.

**Nature of the Data Event**

On July 2, 2018, Arcadia became aware of unusual activity in an employee's email account. Arcadia immediately launched a detailed and exhaustive investigation to determine what happened and what information may have been affected. With the assistance of computer forensics experts, Arcadia learned that credentials for an Arcadia employee's email account were compromised which resulted in unauthorized access to that account on or about February 4, 2018.

Arcadia undertook a lengthy review of the impacted accounts to determine if any information was subject to unauthorized access. When the investigation could not rule out the possibility of such access, Arcadia engaged in a programmatic and manual review of the email accounts to determine if personal information existed in the accounts at the time of the incident. That review concluded on October 20, 2018. Arcadia undertook a lengthy review of their employee, student, and vendor

Attorney General MacDonald  
March 26, 2019  
Page 2

records to confirm address information for the potentially impacted individuals for purposes of providing notification to those individuals.

Arcadia confirmed the email accounts contained personal information relating to three (3) New Hampshire residents including name and Social Security number.

#### **Notice to New Hampshire Residents**

On or about March 26, 2019, Arcadia provided written notice of this incident to affected individuals, which includes three (3) 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**

Upon discovering the event, Arcadia moved quickly to investigate and respond to the incident, assess the security of Arcadia's systems, and notify potentially affected individuals. Arcadia has strict security measures in place to protect information and upon learning of this incident, took additional steps relating to its employee email accounts. Arcadia reset passwords for Arcadia email accounts and is reviewing its existing policies and procedures and also implementing additional technology tools and training to detect and prevent future such incidents. As a precautionary matter, Arcadia notified law enforcement and also provided relevant regulatory notices.

Arcadia is also providing access to identity protection and credit monitoring services for one (1) year, through Kroll, to individuals whose personal information was potentially affected by this incident, at no cost to these individuals.

Additionally, Arcadia is providing impacted individuals with guidance on how to better protect against identity theft and fraud, including advising individuals to report any suspected incidents of identity theft or fraud to their credit card company and/or bank. Arcadia is providing individuals with information on how to place a fraud alert and security freeze on one's credit file, information on protecting against tax 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**

Should you have any questions regarding this notification or other aspects of the data security event, please contact us at (267) 930-4784.

Very truly yours,



Jeffrey J. Boogay of  
MULLEN COUGHLIN LLC

JJB/ajd

# EXHIBIT A



<<Date>> (Format: Month Day, Year)

<<FirstName>> <<MiddleName>> <<LastName>> <<NameSuffix>>  
<<Address1>>  
<<Address2>>  
<<City>>, <<State>> <<Zip>>

## Notice of Data Breach

Dear <<FirstName>> <<LastName>>,

Arcadia University ("Arcadia") writes to inform you of a recent event that may affect the security of some of your personal 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 information about the recent incident, steps we have taken in response, and steps you can take to protect against fraud should you feel it is appropriate.

### What Happened?

On or around July 2, 2018, Arcadia was alerted to suspicious activity related to an employee's email account. Arcadia immediately launched an investigation into the incident to determine the full nature and scope of what occurred. Through its detailed and exhaustive investigation, Arcadia confirmed that an unknown actor(s) gained access to an Arcadia employee's email account. The employee's email credentials were changed, and the email account has been secured. A leading forensic investigation firm was immediately retained to assist with Arcadia's investigation into what happened and what information contained within the email account may be affected. The investigation determined that the account at issue experienced unauthorized access on or about February 4, 2018 but was unable to determine what specific items within the account may have been accessed by the actor(s).

As a result, the contents of the accounts were reviewed through a manual and programmatic process to determine what sensitive data may have been accessible. On October 20, 2018, we confirmed the identities of the individuals who may have had information accessible as a result of the incident and promptly launched a lengthy review of our files to ascertain address information for the impacted individuals.

### What Information Was Involved?

While we currently have no evidence that your information was subject to actual or attempted misuse, we confirmed that your <<ClientDef1(name[ and/, ][DATA ELEMENTS])>><<ClientDef2([DATA ELEMENTS])>> were contained within the affected employee email accounts.

### What We Are Doing.

The confidentiality, privacy, and security of information in our care is one of our highest priorities. Upon learning of this incident, we took steps to secure the affected email account and to find out what happened. As part of our ongoing commitment to the security of the information in our care, we are reviewing our existing policies and procedures and also implementing additional technology tools and training to detect and help prevent future such incidents.

While we have no evidence of any actual or attempted misuse of any of the affected information, we are providing notice of this incident to potentially impacted individuals, including you. We also secured the services of Kroll to provide identity monitoring at no cost to you for one year. Kroll is a global leader in risk mitigation and response, and their team has extensive experience helping people who have sustained an unintentional exposure of confidential data. Your identity monitoring services include Credit Monitoring, Fraud Consultation, and Identity Theft Restoration. Please see below for instructions on enrollment in these identity monitoring services:



Visit [krollbreach.idMonitoringService.com](http://krollbreach.idMonitoringService.com) to activate and take advantage of your identity monitoring services.

You have until **June 20, 2019** to activate your identity monitoring services.

Membership Number: <<Member ID>>

To receive credit services by mail instead of online, please call 1-844-263-8605. Additional information describing your services is included with this letter.

**What you can do.**

You may review the enclosed “[Steps You Can Take to Prevent Identity Theft and Fraud](#)”. You may also enroll to receive the free identity monitoring services described above.


**For More Information.**

We understand you may have questions about this incident that are not addressed in this letter. If you have additional questions, please call 1-866-775-4209, Monday through Friday from 8:00 a.m. to 5:30 p.m. Central Time. Please have your membership number ready.

You may also write to us at Attn: Office of General Counsel, 450 South Easton Road, Glenside, PA 19038.

Arcadia takes the privacy and security of the personal information in our care very seriously. We sincerely regret any inconvenience or concern this incident may cause you.

Sincerely,



Eric R. Nelson  
Vice President for Finance & Treasurer  
Arcadia University

## Steps You Can Take to Protect Against Identity Theft and Fraud

We encourage you to remain vigilant against incidents of identity theft and fraud, to review your account statements, and to monitor your credit reports for suspicious activity. Under U.S. law you are entitled to one free credit report annually from each of the three major credit reporting bureaus. To order your free credit report, visit [www.annualcreditreport.com](http://www.annualcreditreport.com) or call, toll-free, 1-877-322-8228. You may also contact the three major credit bureaus directly to request a free copy of your credit report.

You have the 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. The security freeze is designed to prevent credit, loans, and services from being approved in your name without your consent. However, you should be aware that using a security freeze to take control over who gets access to the personal and financial information in your credit report may delay, interfere with, or prohibit the timely approval of any subsequent request or application you make regarding a new loan, credit, mortgage, or any other account involving the extension of credit. Pursuant to federal law, you cannot be charged to place or lift a security freeze on your credit report. Should you wish to place a security freeze, please contact the major consumer reporting agencies listed below:

<b>Experian</b> PO Box 9554 Allen, TX 75013 1-888-397-3742 <a href="http://www.experian.com/freeze/center.html">www.experian.com/freeze/center.html</a>	<b>TransUnion</b> P.O. Box 2000 Chester, PA 19016 1-888-909-8872 <a href="http://www.transunion.com/credit-freeze">www.transunion.com/credit-freeze</a>	<b>Equifax</b> PO Box 105788 Atlanta, GA 30348-5788 1-800-685-1111 <a href="http://www.equifax.com/personal/credit-report-services">www.equifax.com/personal/credit-report-services</a>
---	---	---

In order to request a security freeze, you will need to provide the following information:

1. Your full name (including middle initial as well as Jr., Sr., II, III, etc.);
2. Social Security number;
3. Date of birth;
4. If you have moved in the past five (5) years, provide the addresses where you have lived over the prior five years;
5. Proof of current address, such as a current utility bill or telephone bill;
6. A legible photocopy of a government-issued identification card (state driver's license or ID card, military identification, etc.);
7. 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.

As an alternative to a security freeze, you have the right to place an initial or extended "fraud alert" on your file at no cost. An initial fraud alert is a 1-year alert that is placed on a consumer's credit file. Upon seeing a fraud alert display on a consumer's credit file, a business is required to take steps to verify the consumer's identity before extending new credit. If you are a victim of identity theft, you are entitled to an extended fraud alert, which is a fraud alert lasting seven years. Should you wish to place a fraud alert, please contact any one of the agencies listed below:

<b>Experian</b> P.O. Box 2002 Allen, TX 75013 1-888-397-3742 <a href="http://www.experian.com/fraud/center.html">www.experian.com/fraud/center.html</a>	<b>TransUnion</b> P.O. Box 2000 Chester, PA 19106 1-800-680-7289 <a href="http://www.transunion.com/fraud-victim-resource/place-fraud-alert">www.transunion.com/fraud-victim-resource/place-fraud-alert</a>	<b>Equifax</b> P.O. Box 105069 Atlanta, GA 30348 1-888-766-0008 <a href="http://www.equifax.com/personal/credit-report-services">www.equifax.com/personal/credit-report-services</a>
---	---	--

Although we have no reason to believe that your personal information has been used to file fraudulent tax returns, you can contact the IRS at [www.irs.gov/Individuals/Identity-Protection](http://www.irs.gov/Individuals/Identity-Protection) for helpful information and guidance on steps you can take to address a fraudulent tax return filed in your name and what to do if you become the victim of such fraud. You can also visit [www.irs.gov/uac/Taxpayer-Guide-to-Identity-Theft](http://www.irs.gov/uac/Taxpayer-Guide-to-Identity-Theft) for more information.

You can further educate yourself regarding identity theft, fraud alerts, security freezes, and the steps you can take to protect yourself, by contacting the consumer reporting agencies, the Federal Trade Commission, or your state Attorney General.

The Federal Trade Commission can be reached at: 600 Pennsylvania Avenue NW, Washington, DC 20580, [www.identitytheft.gov](http://www.identitytheft.gov), 1-877-ID-THEFT (1-877-438-4338); TTY: 1-866-653-4261. The Federal Trade Commission also encourages those who discover that their information has been misused to file a complaint with them. You can obtain further information on how to file such a complaint by way of the contact information listed above. You have the right to file a police report if you ever experience identity theft or fraud. Please note that in order to file a report with law enforcement for identity theft, you will likely need to provide some proof that you have been a victim. Instances of known or suspected identity theft should also be reported to law enforcement and your state Attorney General. This notice has not been delayed by law enforcement.

**For North Carolina residents**, the Attorney General can be contacted at 9001 Mail Service Center, Raleigh, NC 27699-9001, 1-877-566-7226 or 1-919-716-6400, [www.ncdoj.gov](http://www.ncdoj.gov).

**For Maryland residents**, the Attorney General can be contacted at 200 St. Paul Place, 16th Floor, Baltimore, MD 21202, 1-888-743-0023, [www.oag.state.md.us](http://www.oag.state.md.us).

**For 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 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. We encourage you to review your rights pursuant to the Fair Credit Reporting Act by visiting [www.consumerfinance.gov/f/201504\\_cfpb\\_summary\\_your-rights-under-fcra.pdf](http://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.

**For Rhode Island Residents:** The Rhode Island Attorney General can be reached at: 150 South Main Street, Providence, Rhode Island 02903, [www.riag.ri.gov](http://www.riag.ri.gov), 1-401-274-4400. Under Rhode Island law, you have the right to obtain any police report filed in regard to this incident. **There are XXX Rhode Island residents impacted by this incident.**



## TAKE ADVANTAGE OF YOUR IDENTITY MONITORING SERVICES

You've been provided with access to the following services<sup>1</sup> from Kroll:

### Single Bureau Credit Monitoring

You will receive alerts when there are changes to your credit data—for instance, when a new line of credit is applied for in your name. If you do not recognize the activity, you'll have the option to call a Kroll fraud specialist, who can help you determine if it's an indicator of identity theft.

### Fraud Consultation

You have unlimited access to consultation with a Kroll fraud specialist. Support includes showing you the most effective ways to protect your identity, explaining your rights and protections under the law, assistance with fraud alerts, and interpreting how personal information is accessed and used, including investigating suspicious activity that could be tied to an identity theft event.

### Identity Theft Restoration

If you become a victim of identity theft, an experienced Kroll licensed investigator will work on your behalf to resolve related issues. You will have access to a dedicated investigator who understands your issues and can do most of the work for you. Your investigator can dig deep to uncover the scope of the identity theft, and then work to resolve it.

<sup>1</sup> Kroll's activation website is only compatible with the current version or one version earlier of Internet Explorer, Chrome, Firefox, and Safari. To receive credit services, you must be over the age of 18 and have established credit in the U.S., have a Social Security number in your name, and have a U.S. residential address associated with your credit file.