



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

Samuel Sica, III  
Office: (267) 930-4802  
Fax: (267) 930-4771  
Email: [ssica@mullen.law](mailto:ssica@mullen.law)

426 W. Lancaster Avenue, Suite 200  
Devon, PA 19333

February 1, 2021

**VIA E-MAIL**

Office of the Attorney General  
1125 Washington Street SE  
PO Box 40100  
Olympia, WA 98504-0100  
E-mail: [securitybreach@atg.wa.gov](mailto:securitybreach@atg.wa.gov)

**Re: Notice of Data Event**

Dear Sir or Madam:

We represent Gonzaga University (“Gonzaga”) located at 502 E Boone Ave, AD 95, Spokane, WA 99258, and write to notify your office of an incident that may affect the security of some personal information relating to approximately eight thousand forty-one (8,041) residents. This notice may be supplemented if any new significant facts are learned subsequent to its submission. By providing this notice, Gonzaga does not waive any rights or defenses regarding the applicability of Washington law, the applicability of the Washington data event notification statute, or personal jurisdiction.

**Nature of the Data Event**

Gonzaga recently learned of unusual activity related to an employee email account and immediately took steps to secure the account and work with third-party computer forensics specialists to determine the nature and scope of the incident. On August 19, 2020, the investigation confirmed that the Gonzaga employee email account was accessed by an unknown actor on August 6, 2020.

The investigation was unable to determine what emails within the account were accessed by the unauthorized actor. Therefore, in an abundance of caution, Gonzaga worked with third-party specialists to perform a comprehensive review of all information stored in the email account at the time of the incident to confirm the types of information contained in the account and to whom the information related. Upon completion of the third-party review, Gonzaga then conducted a thorough manual review of its records to determine the identities and contact information for potentially impacted individuals. On January 13, 2021, Gonzaga completed its internal review and confirmed contact information for potentially affected individuals.

The review determined the following types of information relating to Washington residents were present in the impacted email account: name, Social Security number, date of birth, driver's license or state identification card number, student identification number, passport number, username and password to an online account, financial account information, credit or debit card number, medical information, and health insurance information.

### **Notice to Washington Residents**

On or about September 10, 2020, Gonzaga began providing written notice of this incident to potentially affected individuals while the investigation was ongoing. On February 1, 2021, upon completion of the review, Gonzaga continued providing written notice to affected individuals, which includes approximately eight thousand forty-one (8,041) Washington 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**

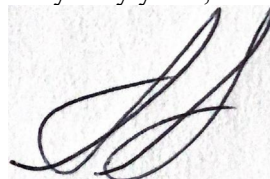
Upon discovering the event, Gonzaga moved quickly to investigate and respond to the incident and to notify potentially affected individuals. As part of Gonzaga's ongoing commitment to the security of personal information in its care, Gonzaga is reviewing its existing policies and procedures to include additional technical and administrative safeguards.

Gonzaga is also providing potentially affected individuals, except those with only student identification number impacted, with complimentary access to twenty-four (24) months of credit monitoring and identity restoration services through Kroll. Additionally, Gonzaga is providing potentially affected 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 financial institution. Gonzaga is also providing individuals with information on how to place a fraud alert and security freeze on one's credit file, 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. Gonzaga notified the U.S. Department of Education and assisted with its investigation into the event. Gonzaga also notified other state regulators, as required.

### **Contact Information**

Should you have any questions regarding this notification or other aspects of the data security event, please contact us at (267) 930-4802.

Very truly yours,

A handwritten signature in black ink, appearing to read 'Sica', is written over a rectangular area that has been redacted with a light gray background.

Samuel Sica, III of  
MULLEN COUGHLIN LLC

# **EXHIBIT A**



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

<<first\_name>> <<middle\_name>> <<last\_name>> <<suffix>>  
<<address\_1>>  
<<address\_2>>  
<<city>>, <<state\_province>> <<postal\_code>>  
<<country >>

<< b2b\_text\_1(Subject Line)>>

Dear <<first\_name>> <<middle\_name>> <<last\_name>> <<suffix>>,

Gonzaga University (“Gonzaga”) is writing to inform you of a recent event that may impact the security of some of your personal information. While we are unaware of any attempted or actual misuse of your information, we are providing you with information about the event, our response, and steps you may take to help protect your information should you feel it is necessary to do so.

**What Happened?** Gonzaga recently learned of unusual activity related to an employee email account and immediately took steps to secure the account and work with a computer forensics specialist to determine the nature and scope of the incident. On August 19, 2020, the investigation confirmed that the Gonzaga employee email account was accessed by an unknown actor on August 6, 2020.

The investigation was unable to determine what emails within the account were accessed by the unauthorized actor. Therefore, in an abundance of caution, we began a comprehensive review of all information stored in the email account at the time of the incident to confirm the types of information contained in the account and to whom the information related. Upon completion of the third-party review, we then conducted a thorough manual review of our records to determine the identities and contact information for potentially impacted individuals. On January 13, 2021, we completed our internal review and confirmed contact information for potentially affected individuals.

**What Information was Involved?** We determined the following types of information relating to you were present in the impacted email account at the time of the event: << b2b\_text\_2(Data Elements)>>. We have no indications of misuse of your information, and Gonzaga is providing this notice in an abundance of caution.

**What We Are Doing.** We take this incident and the security of personal information in our care seriously. Upon learning of this incident, we immediately took steps to secure the affected email account and conduct an investigation. As part of our ongoing commitment to the security of personal information in our care, we are reviewing our existing policies and procedures to include additional safeguards. We also notified government regulators, as required. Although we are unaware of any misuse of your information as a result of this incident, we are offering you access to 24 months of complimentary identity monitoring services through Kroll.

**What You Can Do.** You can find out more about how to protect your information in the enclosed *Steps You Can Take to Help Protect Your Information*. We encourage you to remain vigilant against incidents of identity theft and fraud, to review your account statements and credit reports for unusual activity, and to report any suspicious activity immediately to your bank or financial institution. You may also activate the complimentary identity monitoring services described above. Activation instructions are attached to this letter.

**For More Information.** If you have additional questions, please call us at 1-877-461-2596, Monday through Friday (excluding U.S. holidays), during the hours of 6:00 a.m. to 3:30 p.m., Pacific Time. You may also write to Gonzaga University at 502 E Boone Ave, AD 95, Spokane, WA 99258.

We sincerely regret any inconvenience or concern this incident may cause.

Sincerely,

*Borre B. Ulrichsen*

Borre Ulrichsen

Chief Information Officer

Gonzaga University

## **STEPS YOU CAN TAKE TO HELP PROTECT YOUR INFORMATION**

### **Activation Instructions**

To help relieve concerns and restore confidence following this incident, we have secured the services of Kroll to provide identity monitoring services at no cost to you for 24 months. 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.

Visit <https://enroll.idheadquarters.com> to activate and take advantage of your identity monitoring services.

You have until <<Date>> to activate your identity monitoring services.

Membership Number: <<Member ID>>

Additional information describing your services is included with this letter.

### **Monitor Your Accounts**

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:

#### **Experian**

P.O. Box 9554  
Allen, TX 75013  
1-888-397-3742  
[www.experian.com/freeze/center.html](http://www.experian.com/freeze/center.html)

#### **TransUnion**

P.O. Box 160  
Chester, PA 19016  
1-888-909-8872  
[www.transunion.com/credit-freeze](http://www.transunion.com/credit-freeze)

#### **Equifax**

P.O. Box 105788  
Atlanta, GA 30348-5788  
1-800-685-1111  
[www.equifax.com/personal/credit-report-services](http://www.equifax.com/personal/credit-report-services)

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, 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, 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:

#### **Experian**

P.O. Box 9554  
Allen, TX 75013  
1-888-397-3742  
[www.experian.com/fraud/center.html](http://www.experian.com/fraud/center.html)

#### **TransUnion**

P.O. Box 2000  
Chester, PA 19016  
1-800-680-7289  
[www.transunion.com/fraud-victim-resource/place-fraud-alert](http://www.transunion.com/fraud-victim-resource/place-fraud-alert)

#### **Equifax**

P.O. Box 105069  
Atlanta, GA 30348  
1-888-766-0008  
[www.equifax.com/personal/credit-report-services](http://www.equifax.com/personal/credit-report-services)

## **Additional 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); and 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 Maryland residents:** The Attorney General may be contacted at 200 St. Paul Place, 16th Floor, Baltimore, MD 21202; 1-410-528-8662; and [www.oag.state.md.us](http://www.oag.state.md.us).

**For North Carolina residents:** The Attorney General may be contacted at 9001 Mail Service Center, Raleigh, NC 27699-9001; 1-877-566-7226 or 1-919-716-6000; and [www.ncdoj.gov](http://www.ncdoj.gov). You can obtain information from the Attorney General or the Federal Trade Commission about preventing identity theft.

**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 Attorney General may be contacted at: 150 South Main Street, Providence, Rhode Island 02903; [www.riag.ri.gov](http://www.riag.ri.gov); and 1-401-274-4400. Under Rhode Island law, you have the right to obtain any police report filed in regard to this incident. There is [one \(1\)](#) Rhode Island resident impacted by this incident.

**For New York residents:** The Attorney General may be contacted at: Office of the Attorney General, The Capitol, Albany, NY 12224-0341; 1-800-771-7755; and <https://ag.ny.gov/>

## **TAKE ADVANTAGE OF YOUR IDENTITY MONITORING SERVICES**

You have been provided with access to the following services 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 will have the option to call a Kroll fraud specialist, who will be able to help you determine if it is 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 will be able to dig deep to uncover the scope of the identity theft, and then work to resolve it.