NELSON MULLINS

NELSON MULLINS RILEY & SCARBOROUGH LLP
ATTORNEYS AND COUNSELORS AT LAW

201 17th Street NW, Suite 1700
Atlanta, GA 30363
T: 404.322.6000 F: 404.322.6050
nelsonmullins.com

Gina G. Greenwood
T: 478.387.0458
gina.greenwood@nelsonmullins.com

October 2, 2023

Attorney General Anthony Brown
200 St. Paul Place
Baltimore MD 21202
idtheft@oag.state.md.us

RE: *Point University - Notice of Data Incident*

Dear Attorney General Brown:

I serve as outside legal counsel to Point University ("Point"), which is a private university with its principal office located at 507 West 10th Street, West Point, GA 31833.[1]

This correspondence is to notify you of a recent security incident at Point involving the inadvertent disclosure of a single electronic file containing sensitive personal information of a limited number of Point students. Specifically, on or about August 8, 2023, Point was made aware that two (2) current students of the University were unintentionally granted access to the file, which was stored on the University's secure SharePoint platform, due to a suspected, inadvertent configuration error and that the two students had viewed the file on or about August 7, 2023.

Upon discovery of this incident, Point immediately began an investigation and blocked the unintended access to the document. Third-party experts were also engaged to assist. While the investigation is ongoing, preliminary findings indicate no other unauthorized individuals accessed the file and no unauthorized downloads of the file occurred. While Point has no evidence of any misuse of anyone's personal information as a result of this incident, the University conducted a thorough review of the impacted data to determine whether sensitive information was present and to identify individuals whose information may have been involved. Through these efforts, Point determined that information regarding a resident of your State may have been impacted by this incident.

In an abundance of caution, notification letters began going out via U.S. Mail to 1 resident of your State on or about October 4, 2023. The notification letter includes instructions for activating credit monitoring services at no cost to the recipient. The PII that was potentially

[1] By providing this notice, Point University does not waive any rights or defenses regarding the applicability of Maryland law, the applicability of the Maryland data event notification statute, or personal jurisdiction.

at risk included first and last name, Social Security number, student ID number, academic program information, enrollment status, and/or academic progress status.

A sample notification letter is enclosed for your reference and includes:

- A description of the security event;
- Steps taken to investigate;
- Steps taken to mitigate any potential harm to consumers;
- Instructions for activating free identity theft protection services that include credit monitoring and a $1 million insurance reimbursement policy to all consumers who received notification;
- Instructions on how to place a security freeze on the recipient's consumer credit report; and
- Instructions regarding how to obtain more information about this event, etc.

Point is fully committed to protecting consumer privacy and the confidentiality of personal information. To that end, Point has a written information security policy. We will follow-up this correspondence with any forms or other documents that may need to be completed. Please contact me if you require any additional information regarding this incident.

Very truly yours,

/s/ Gina G. Greenwood
Gina G. Greenwood

GGG:aps

Point University

Secure Processing Center
P.O. Box 3826
Suwanee, GA 30024

<<MailID>>
<<Name 1>>
<<Name 2>>
<<Address 1>>
<<Address 2>>
<<Address 3>>
<<Address 4>>
<<City>><<State>><<Zip>>
<<Country>>

<<Date>>

Re: Notice of Data <<Variable>>

Dear <<Name 1>>:

I am writing to notify you of a recent incident that may have involved some of your personal information and to provide you with information regarding steps you may wish to take.

What Happened? On or about August 8, 2023, Point University (the "University") was made aware of an incident involving certain limited information stored within a single spreadsheet on the University's secure SharePoint platform. Specifically, due to an unknown and unintentional configuration error, it appears the file and some individuals' information contained within it was temporarily and inadvertently accessible to others. Immediately upon discovery, the University blocked the unintended access to such information and began an investigation to determine the full nature and scope of the incident.

What Information Was Involved? Following the investigation, the University has determined that some of your personal information may have been contained within the affected file, including your name, social security number, student ID number, academic program information, enrollment status, and/or academic progress status. Although the University currently has no evidence that any of your personal information has been misused, the University is providing this information to you out of an abundance of caution to ensure you are aware of this incident.

What We Are Doing and What You Can Do. Moreover, while we are not aware of any fraud at this time, for your peace of mind, we are offering you **<<CM Duration>> of free credit monitoring and identity theft protection through Experian**. **<u>You must activate the free product in order for it to be effective</u>.** The activation instructions are included with this notification. We also have included some additional steps that you can take to protect yourself as you deem appropriate.

For more information about this incident, please call 855-455-6959 between 9:00 A.M and 9:00 P.M. Eastern Time, Monday - Friday (excluding major U.S. holidays). Information privacy and security are among the University's highest priorities, and we are fully committed to protecting your personal information. We apologize for any inconvenience or concern this may have caused.

Sincerely,

Point University

STEPS YOU CAN TAKE

Below is information on steps you can take to protect yourself, if you feel it necessary under the circumstances.

➢ **ACTIVATE Your FREE Experian IdentityWorks Product NOW in Three Easy Steps.** To help protect your identity, we are offering you a **complimentary 12-month membership** to Experian's IdentityWorks product. This product helps detect possible future misuse of your personal information and provides you with superior identity protection support focused on immediate identification and resolution of identity theft. IdentityWorks Alert is completely free to you and enrolling in this program will not hurt your credit score.

1. **ENSURE You Enroll By**: **December 8, 2023 (Your code will not work after this date.)**
2. **VISIT** the **Experian IdentityWorks website** to enroll: https://www.experianidworks.com/3bcredit
3. **PROVIDE Your Activation Code**: **<<activation code>>**

If you have questions about the IdentityWorks or need an alternative to enrolling online, **please call 800-459-4631** and provide engagement **<<engagement code>>.** A credit card is not required for enrollment.

Once your IdentityWorks membership is activated, you will receive the following features:

- **Experian Credit Report at Signup:** See what information is associated with your credit file. Daily credit reports are available for online members only.[1]
- **Credit Monitoring:** Actively monitors Experian file for indicators of fraud.
- **Identity Restoration:** Restoration Agents are immediately available to help address credit/non-credit related fraud.
- **$1 Million Identity Theft Insurance:**[2] Provides coverage for certain costs and unauthorized electronic fund transfers.

You must activate your membership by the Enrollment Date (noted above) by enrolling at https://www.experianidworks.com/3bcredit or calling 877-288-8057 to register your activation code above in order for this service to be activated. Once your enrollment in IdentityWorks is complete, carefully review your credit report for inaccurate or suspicious items. 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 team at 877-288-8057.

Additional Steps You May Wish to Take:

➢ **FREEZE YOUR CREDIT FILE.** 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. A security freeze is designed to prevent credit, loans, and services from being approved in your name without your consent. However, using a freeze to take control over who gets access to the personal/financial information in your credit report may delay, interfere with, or prohibit the timely approval of any subsequent request or application made regarding a new loan, credit, mortgage, or any other account involving extension of credit. Security freeze generally does not apply to existing account relationships and when a copy of your report is requested by existing creditor or its agents or affiliates for certain types of account review, collection, fraud control or similar activities. There is no charge to place or lift a freeze. To place a security freeze on your credit report, contact each of the following credit bureaus and clearly explain in the call/letter that you are requesting a security freeze:

- *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

---

[1] Offline members will be eligible to call for additional reports quarterly after enrolling.

2 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.

To request a security freeze, provide your full name (middle initial, Jr., Sr., II, III, etc.), Social Security Number, date of birth; home addresses over the past 5 years; proof of current address such as a current utility bill or telephone bill; photocopy of government issued identification card (driver's license or ID card, military ID, etc.); and 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. If you request a security freeze via toll-free telephone or other secure electronic means, credit reporting agencies have 1 business day after receiving the request to place the freeze. In the case of a request made by mail, the agencies have 3 business days after receiving your request to place a security freeze on your credit report. Credit agencies must also send written confirmation within 5 business days and provide a unique personal identification number (PIN) or password, or both that can be used to authorize the removal or lifting of the security freeze. To lift the freeze to allow a specific entity or individual access to your credit report, you must call or send a written request to the credit reporting agencies by mail and include proper identification (name, address, and social security number) and PIN or password provided when you placed the security freeze as well as the identities of those entities or individuals you would like to receive your credit report or the specific period of time you want the credit report available. The credit reporting agencies have 3 business days after receiving a request to lift freeze for those identified entities or for the specified period of time. To remove the freeze, you must send a written request to the 3 credit bureaus by mail and include proper identification (name, address, & social security number) and PIN number or password provided when you placed the freeze. The credit bureaus have 3 business days after receiving the request to remove the freeze.

- **PLACE FRAUD ALERTS ON YOUR CREDIT FILE.** As an alternative to a security freeze, you have the right to place an initial or extended fraud alert on your credit 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 an alert lasting 7 years. Contact the 3 credit reporting agencies listed above to activate an alert.

- **REMAIN VIGILANT: REVIEW YOUR ACCOUNT STATEMENTS & REPORT FRAUD. CHANGE PASSWORDS AND SECURITY VERIFICATION QUESTIONS & ANSWERS.** Carefully review your credit reports, debit/credit card, insurance policy, bank account and other account statements. Activate alerts on your bank accounts to notify you of suspicious activity, changing passwords/security verifications as needed – particularly if same password is used over multiple online accounts. If your medical information was involved, it is also advisable to review the billing statements you receive from your healthcare providers. Report suspicious or fraudulent charges to your insurance statements, provider billing statements, credit report, credit card or bank accounts to your insurance company, bank/credit card vendor, healthcare provider and law enforcement, including FTC and/or your State Attorney General.

- **ORDER YOUR FREE ANNUAL CREDIT REPORTS.** Visit www.annualcreditreport.com or call 877-322-8228 to obtain 1 free copy of your credit report annually. Periodically review a copy of your credit report for discrepancies and identify accounts you did not open or inquiries you did not authorize. (For Colorado, Maine, Maryland, Massachusetts, New Jersey, Puerto Rico, and Vermont residents: You may obtain additional copies of your credit report, free of charge. You must contact each of the 3 credit reporting agencies directly to obtain such additional reports.) –

    - *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

- **FAIR CREDIT REPORTING ACT (FCRA):** 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. 1) You must be told if information in your file has been used against you. 2) You have the right to know what is in your file. 3) You have the right to ask for a credit score. 4) You have the right to dispute incomplete or inaccurate information. 5) Consumer reporting agencies must correct or delete inaccurate, incomplete, or unverifiable information. 6) Consumer reporting agencies may not report outdated negative information. 7) Access to your file is limited. 8) You must give your consent for reports to be provided to employers. 9) You may limit "prescreened" offers of credit and insurance you get based on information in your credit report. 10) 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. 11) You may seek damages from violators. 12) Identity theft victims and active-duty military personnel have additional rights.

- **OBTAIN INFORMATION ABOUT PREVENTING IDENTITY THEFT, FRAUD ALERTS, SECURITY FREEZES AND FCRA FROM THE FEDERAL TRADE COMMISSION.** Go to http://www.experian.com/credit-advice/topic-fraud-and-identity-theft.html. Federal Trade Commission also provides information at www.ftc.gov/idtheft FTC hotline is 877-438-4338; TTY: 1-866-653-4261 or write to FTC, 600 Pennsylvania Ave., NW, Washington, D.C. 20580.

- **OBTAIN INFORMATION ABOUT PREVENTING IDENTITY THEFT FROM YOUR STATE ATTORNEY GENERAL.** You may contact and obtain information from your state attorney general at:

  - **Maryland Residents**: The Attorney General can be contacted at Office of Attorney General, 200 St. Paul Place, Baltimore, MD 21202; (888) 743-0023; or http://www.oag.state.md.us.
  - **Massachusetts Residents**: Under Massachusetts law, you have the right to obtain any police report filed in connection to the incident. If you are the victim of identity theft, you also have the right to file a police report and obtain a copy of it. Notification of this incident has not been delayed as a result of a law enforcement investigation
  - **North Carolina Residents**: The Attorney General can be contacted at 9001 Mail Service Center, Raleigh, NC 27699- 9001; (919) 716-6400; or http://www.ncdoj.gov.