KING & SPALDING

King & Spalding LLP
1180 Peachtree Street N.E.
Atlanta, GA 30309-3521
Tel: +1 404 572 4600
Fax: +1 404 572 5100
www.kslaw.com

Phyllis B. Sumner
Direct Dial: +1 404 572 4799
Direct Fax: +1 404 572 5100
psumner@kslaw.com

November 17, 2023

Aaron Frey, Attorney General of Maine
6 State House Station
Augusta, ME 04333

Re: Notice of Security Incident Affecting University of Miami

Dear Attorney General Frey,

We write on behalf of University of Miami ("UM") regarding a security incident.

On October 18, 2023, UM discovered that the personal information of a limited number of individuals was inadvertently disclosed on UM's Faculty Senate website. The inadvertent disclosure consisted of a .pdf copy of a Faculty Senate "Memorandum," which contained a petition signed by former UM students. UM immediately took down access to the website upon discovery of the incident. We have confirmed that this inadvertent exposure did not impact any UM systems, nor was this incident the result of malicious cyber activity by third-party hackers.

According to our investigation, the information involved included the individuals' first and last name, and social security number.

As soon as UM became aware of the incident, it took immediate action to investigate and contain the situation, including removing the information from the impacted website, and notifying affected individuals. On November 17, 2023, UM will begin mailing notifications to the affected individuals and offering them two years of identity monitoring services, including Credit Monitoring, Fraud Consultation, and Identity Theft Restoration. We have identified 1 Maine resident who may have been affected by the incident.

An unaddressed copy of the individual letter is attached. UM has also established a call center to answer individuals' questions ((866) 846-0829).

UM remains committed to protecting personal information and assisting those who may have been affected by this incident. UM is providing notices to individuals pursuant to applicable state laws and regulations. By virtue of this notice, UM does not waive any rights and reserves all rights under such laws. Please do not hesitate to contact me if you have any questions regarding this letter.

Very truly yours,

Phyllis B. Sumner

Enclosure

UNIVERSITY OF MIAMI

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

<<first_name>> <<middle_name>> <<last_name>> <<suffix>>
<<address_1>>
<<address_2>>
<<city>>, <<state_province>> <<postal_code>>
<<country>>

Notice of Security Incident

Dear <<b2b_text_1 (Salutation Mr./Ms/Mrs./Dr.)>> <<first_name>> <<middle_name>> <<last_name>> <<suffix>>,

We are writing to alert you of a security incident that may have affected some of your personal information. The University of Miami respects your privacy and we want you to understand what happened, the steps we are taking to address this issue, and what measures you can take to help protect your personal information.

What happened?

The University of Miami recently discovered that some of your personal information was inadvertently disclosed on the University of Miami's Faculty Senate website. The inadvertent disclosure consisted of a .pdf copy of a Faculty Senate "Memorandum," which contained a petition signed by a limited number of former University of Miami students. The University of Miami became aware of the disclosure on October 18, 2023, and immediately took down access to the website.

We have confirmed that this inadvertent exposure did not impact any University of Miami systems, nor was this incident the result of malicious cyber activity by third-party hackers.

What information was involved?

According to our investigation, the information involved may include your first and last name, and your Social Security number.

What we are doing.

The University takes your privacy and security of personal information seriously. As soon as we became aware of the incident, we took immediate action to investigate and contain the situation, including removing the information from the impacted website, and notifying you.

To help relieve concerns and restore confidence following this incident, we have secured the services of Kroll to provide identity monitoring at no cost to you for two years. 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.krollmonitoring.com** to activate and take advantage of your identity monitoring services.

You have until <<b2b_text_6 (activation date)>> to activate your identity monitoring services.

Membership Number: **<<Membership Number s_n>>**

For more information about Kroll and your Identity Monitoring services, you can visit info.krollmonitoring.com.

Additional information describing your services is included with this letter.

What you can do.

Please review the enclosed "Additional Resources" section included with this letter. This section describes additional steps you can take to help protect yourself, including recommendations by the Federal Trade Commission regarding identity theft protection and details on how to place a fraud alert or a security freeze on your credit file.

The University of Miami is committed to data protection. We regularly review our physical and electronic safeguards to protect personal information, and we will continue to take appropriate steps to safeguard personal information and our systems.

For more information.

If you have questions, please call TFN, Monday through Friday from 8:00 a.m. to 5:30 p.m. Central Time, excluding major U.S. holidays. Please have your membership number ready.

On behalf of the University of Miami, we deeply regret any inconvenience or concern this may have caused. Protecting your information is important to us. We trust that the services we are offering to you demonstrate our continued commitment to your security and satisfaction.

Sincerely,

The University of Miami

ADDITIONAL RESOURCES

Contact information for the three nationwide credit reporting agencies:

Equifax, PO Box 740241, Atlanta, GA 30374, www.equifax.com, 1-800-685-1111

Experian, PO Box 2104, Allen, TX 75013, www.experian.com, 1-888-397-3742

TransUnion, PO Box 2000, Chester, PA 19016, www.transunion.com, 1-800-888-4213

Free Credit Report. It is recommended that you remain vigilant by reviewing account statements and monitoring your credit report for unauthorized activity, especially activity that may indicate fraud and identity theft. You may obtain a copy of your credit report, free of charge, once every 12 months from each of the three nationwide credit reporting agencies.

To order your annual free credit report please visit **www.annualcreditreport.com** or call toll free at **1-877-322-8228**.

You can also order your annual free credit report by mailing a completed Annual Credit Report Request Form (available from the U.S. Federal Trade Commission's ("FTC") website at www.consumer.ftc.gov) to:

Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA 30348-5281.

For Colorado, Georgia, Maine, Maryland, Massachusetts, New Jersey, Puerto Rico, and Vermont residents: You may obtain one or more (depending on the state) additional copies of your credit report, free of charge. You must contact each of the credit reporting agencies directly to obtain such additional report(s).

Fraud Alerts. There are two types of 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 at least one year. You may have an extended alert placed on your credit report if you have already been a victim of identity theft and you have the appropriate documentary proof. An extended fraud alert stays on your credit report for seven years. You can place a fraud alert on your credit report by contacting any of the three national credit reporting agencies.

Security Freeze. You have the ability to place a security freeze, also known as a credit freeze, on your credit report free of charge.

A security freeze is intended to prevent credit, loans and services from being approved in your name without your consent. To place a security freeze on your credit report, you may use an online process, an automated telephone line, or submit a written request to any of the three credit reporting agencies listed above. The following information must be included when requesting a security freeze (note that, if you are requesting a credit report for your spouse, this information must be provided for him/her as well): (1) full name, with middle initial and any suffixes; (2) Social Security number; (3) date of birth; (4) current address and any previous addresses for the past 5 years; and (5) any applicable incident report or complaint with a law enforcement agency or the Registry of Motor Vehicles. The request must also include a copy of a government-issued identification card and a copy of a recent utility bill or bank or insurance statement. It is essential that each copy be legible, and display your name, current mailing address, and the date of issue.

Federal Trade Commission and State Attorneys General Offices. 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 home state. You may also contact these agencies for information on how to prevent or minimize the risks of identity theft.

You may contact the **Federal Trade Commission**, Consumer Response Center, 600 Pennsylvania Avenue, NW, Washington, DC 20580, www.ftc.gov/bcp/edu/microsites/idtheft/, 1-877-IDTHEFT (438-4338).

For Maryland residents: You may contact the Maryland Office of the Attorney General, Consumer Protection Division, 200 St. Paul Place, Baltimore, MD 21202, www.oag.state.md.us, 1-888-743-0023.

For North Carolina residents: You may contact the North Carolina Office of the Attorney General, Consumer Protection Division, 9001 Mail Service Center, Raleigh, NC 27699-9001, www.ncdoj.gov, 1-877-566-7226.

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; https://ag.ny.gov/.

For Connecticut residents: You may contact the Connecticut Office of the Attorney General, 165 Capitol Avenue, Hartford, CT 06106, 1-860-808-5318, www.ct.gov/ag.

For Massachusetts residents: You may contact the Office of the Massachusetts Attorney General, 1 Ashburton Place, Boston, MA 02108, 1-617-727-8400, www.mass.gov/ago/contact-us.html

Reporting of identity theft and obtaining a police report.

For Iowa residents: You are advised to report any suspected identity theft to law enforcement or to the Iowa Attorney General.

For Massachusetts residents: You have the right to obtain a police report if you are a victim of identity theft.

For Oregon residents: You are advised to report any suspected identity theft to law enforcement, the Federal Trade Commission, and the Oregon Attorney General.

KROLL

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'll 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.

Kroll's activation website is only compatible with the current version or one version earlier of Chrome, Firefox, Safari and Edge.

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.