



Anjali C. Das
312.821.6164 (direct)
Anjali.Das@wilsonelser.com

June 20, 2024

Via Email: Idtheft@oag.state.md.us

Attorney General Anthony Brown
Office of the Attorney General
Identity Theft Unit
200 St. Paul Place
Baltimore, MD 21202

Re: Notice of Data Incident Involving Indiana University Foundation

Dear Attorney General Brown:

Wilson Elser Moskowitz Edelman and Dicker LLP (“Wilson Elser”) represents Indiana University Foundation (“IUF”), a not-for-profit fundraising organization located at 1500 N. State Road 46 Bypass, Bloomington, IN 47408, with respect to a recent cybersecurity incident that was discovered by IUF on May 1, 2024 (hereinafter, the “incident”). IUF takes the security and privacy of the information within its control very seriously and has taken steps to prevent a similar incident from occurring in the future.

This letter will serve to inform you of the nature of the incident, what information may have been compromised, the number of Maryland residents being notified, and the steps that IUF has taken in response to the incident. We have also enclosed hereto a sample of the notification made to the potentially impacted individuals, which includes an offer of free credit monitoring services.

1. Nature of the Incident

On May 1, 2024, IUF detected suspicious activity linked to an employee’s personal email account. Upon discovery of this incident, IUF immediately secured the account and promptly engaged the IUF’s internal IT Security team to conduct a comprehensive investigation to determine the nature and scope of the incident. Initial forensic investigation determined that an IUF employee’s email account was compromised by an unauthorized actor. The email account has since been secured and remediated. On May 21, 2024, IUF identified individuals whose personal information was contained in the compromised email account. IUF mailed notices to affected individuals on June 20, 2024.

Although IUF is unaware of any fraudulent misuse of information, it is possible that individuals’ full name, address, and Social Security Number may have been exposed as a result of the incident.

55 West Monroe Street, Suite 3800 • Chicago, IL 60603 • p 312.704.0550 • f 312.704.1522

Alabama • Albany • Atlanta • Austin • Baltimore • Beaumont • Boston • Chicago • Dallas • Denver • Edwardsville • Garden City • Hartford • Houston
Indiana • Kentucky • Las Vegas • London • Los Angeles • Miami • Michigan • Milwaukee • Mississippi • Missouri • Nashville • New Jersey • New Orleans
New York • Orlando • Philadelphia • Phoenix • San Diego • San Francisco • Sarasota • Stamford • Virginia • Washington, DC • Wellington • White Plains

wilsonelser.com

As of this writing, IUF has not received any reports of related identity theft since the date of the incident (May 1, 2024, to present).

2. Number of Maryland residents affected.

Based upon the investigation, IUF identified and notified one (1) Maryland resident whose information was impacted as a result of the incident. A notification letter to this affected individual was mailed on June 20, 2024, by U.S. First Class Mail. A sample notification letter is attached hereto as **Exhibit A**.

3. Steps taken in response to the Incident.

Data privacy and security is among IUF's highest priorities, and we are committed to doing everything we can to protect the privacy and security of the personal information in our care. Since the discovery of the incident, IUF moved quickly to investigate, respond, and confirm the security of our systems. Specifically, IUF worked with its internal IT team to secure the compromised account, updated associated user credentials, delete IUF data from the compromised mailbox, and identify which emails may have been compromised. Following the incident, IUF posted an announcement urging employees to purge IUF and Indiana University ("IU") data from any unsecure or personal, non-IUF email accounts. IUF has also enhanced security measures, implemented additional mandatory employee training around the proper handling of IUF/IU data, and will continue to take steps to mitigate the risk of future harm.

IUF is also offering twelve (12) months of complimentary credit monitoring and identity theft restoration services through CyberScout, a TransUnion company, to all affected Maryland residents to help protect their identity. Additionally, IUF provided guidance on how to better protect against identity theft and fraud, including providing 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 the contact details for the Federal Trade Commission.

4. Contact information

IUF remains dedicated to protecting the sensitive information in its control. If you have any questions or need additional information, please do not hesitate to contact me at Anjali.Das@WilsonElser.com or 312-821-6164.

Very truly yours,

Wilson Elser Moskowitz Edelman & Dicker LLP



Anjali C. Das

EXHIBIT A



0000201

Indiana University Foundation
c/o Cyberscout
555 Monster Rd SW
Renton, WA 98057
DB-09024



0_0000201



INDIANA UNIVERSITY
FOUNDATION

[REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]

June 20, 2024

Via First-Class Mail

Re: Notice of Data Security Incident Involving Indiana University Foundation

Dear [REDACTED],

Indiana University Foundation (“IUF”) is writing to inform you of a recent data security incident that may have resulted in an unauthorized access to your deceased family member’s sensitive personal information. While IUF has no evidence that any of your family member’s personal information was compromised or misused in any manner, we are taking appropriate precautionary measures to ensure their financial security and help alleviate concerns you may have.

What Happened?

On May 1, 2024, IUF detected suspicious activity linked to an employee’s personal email account. Upon discovery of this incident, IUF immediately secured the account and promptly engaged the IUF’s internal IT Security team to conduct a comprehensive investigation to determine the nature and scope of the incident. Initial forensic investigation determined that an IUF employee’s email account was compromised by an unauthorized actor. The email account has since been secured and remediated. On May 21, 2024, IUF identified individuals whose personal information was contained in the compromised email account.

What Information Was Involved?

Although IUF has no evidence that any sensitive information has been misused by third parties as a result of this incident, we are notifying you out of an abundance of caution and for purposes of full transparency. Based on the investigation, the following information about your family member may have been subject to unauthorized access: a [REDACTED] with your family member’s name, address, and Social Security Number.

What We Are Doing

Data privacy and security is among IUF's highest priorities, and we are committed to doing everything we can to protect the privacy and security of the personal information in our care. Since the discovery of the incident, IUF moved quickly to investigate, respond, and confirm the security of our systems. Specifically, IUF worked with its internal IT team to secure the compromised account, updated associated user credentials, delete IUF/IU data from the compromised mailbox, and identify which emails may have been compromised. Following the incident, IUF posted an announcement urging employees to purge IUF and Indiana University ("IU") data from any unsecure or personal, non-IUF email accounts. IUF has also enhanced security measures, implemented additional mandatory employee training around the proper handling of IUF/IU data, and will continue to take steps to mitigate the risk of future harm.

To assist you in protecting your family member's information, we are providing you with access to **Cyber Monitoring** services for your deceased family member at no charge. These services provide you with alerts for twelve months from the date of enrollment. Cyber monitoring will look out for your family member's personal data on the dark web and alert you if their personally identifiable information is found online. These services will be provided by Cyberscout, a TransUnion company specializing in fraud assistance and remediation services.

What You Can Do

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 or unauthorized activity. Additionally, security experts suggest that you contact your financial institution and all major credit bureaus to inform them of such a breach and then take whatever steps are recommended to protect your interests, including the possible placement of a fraud alert on your credit file. Please review the enclosed *Steps You Can Take to Help Protect Your Information*, to learn more about how to protect against the possibility of information misuse.

How do I enroll for the free services?

To enroll your family member in Cyber Monitoring services at no charge, please log on to <https://bfs.cyberscout.com/activate> and follow the instructions provided. When prompted please provide the following unique code to receive services: XXXXXXXXXX

In order for you to receive the monitoring services described above, you must enroll within 90 days from the date of this letter. The enrollment requires an internet connection and e-mail account and may not be available to minors under the age of 18 years of age. Please note that when signing up for monitoring services, you may be asked to verify personal information for your own protection to confirm your identity.

We would like to reiterate that, at this time, there is no evidence that your family member's personal information was misused. However, we encourage you to take full advantage of the services offered.

For More Information

Representatives are available for 90 days from the date of this letter, to assist you with questions regarding this incident, between the hours of 8:00 am to 8:00 pm Eastern time, Monday through Friday. Please call the help line [REDACTED] and supply the fraud specialist with your unique code listed above.

At IUF we take our responsibilities to protect our client's personal information very seriously. We are deeply disturbed by this situation and apologize for any inconvenience.

Sincerely,



Philippa M. Guthrie
EVP, General Counsel, Corporate Board Secretary
Indiana University Foundation

Steps You Can Take to Help Protect Your Information

Credit Reports: You may obtain a copy of your credit report, free of charge, whether or not you suspect any unauthorized activity on your account. You may obtain a free copy of your credit report from each of the three nationwide credit reporting agencies. To order your 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 at <https://www.consumer.ftc.gov/articles/0155-free-credit-reports>) to: Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA, 30348-5281.

Fraud Alerts: You can place fraud alerts with the three credit bureaus by phone or online. A fraud alert tells creditors to follow certain procedures, including contacting you, before they open any new accounts or change your existing accounts. For that reason, placing a fraud alert can protect you, but also may delay you when you seek to obtain credit. As of September 21, 2018, initial fraud alerts last for one year. Victims of identity theft can also get an extended fraud alert for seven years.

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-alerts

Equifax
P.O. Box 105069
Atlanta, GA 30348
1-800-525-6285
[https://www.equifax.com/personal/
credit-report-services/
credit-fraud-alerts/](https://www.equifax.com/personal/credit-report-services/credit-fraud-alerts/)

Monitoring: You should always remain vigilant for incidents of fraud and identity theft by reviewing credit card account statements and by monitoring your credit report for suspicious or unusual activity.

Security Freeze: You have the right to place a security freeze on your credit report. 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 need to make a request to each consumer reporting agency. You may make that request by certified mail, overnight mail, regular stamped mail, or by following the instructions found at the websites listed below. The following information must be included when requesting a security freeze (note that if you are requesting a credit report for your spouse or a minor under the age of 16, 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 five 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, display your name and current mailing address, and the date of issue. As of September 21, 2018, it is free to place, lift, or remove a security freeze. You may also place a security freeze for children under the age of 16. You may obtain a free security freeze by contacting any one or more of the following national consumer reporting agencies:

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
Woodlyn, PA 19094
1-888-909-8872
www.transunion.com/credit-freeze

Equifax
P.O. Box 105788
Atlanta, GA 30348-5788
1-888-298-0045
[https://www.equifax.com/personal/
credit-report-services/
credit-freeze/](https://www.equifax.com/personal/credit-report-services/credit-freeze/)

File Police Report: You have the right to file or obtain a police report if you experience identity fraud. Please note that in order to file a crime report or incident report with law enforcement for identity theft, you will likely need to provide proof that you have been a victim. A police report is often required to dispute fraudulent items. You can generally report suspected incidents of identity theft to local law enforcement or to the Attorney General.

FTC and Attorneys General: 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, 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. Instances of known or suspected identity theft should also be reported to law enforcement.

For residents of Iowa: State law advises you to report any suspected identity theft to law enforcement or to the Attorney General.

For residents of Massachusetts: It is required by state law that you are informed of your right to obtain a police report filed in regard to this 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.

For residents of New Mexico: State law advises you to review personal account statements and credit reports, as applicable, to detect errors resulting from the security breach. 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 violators. 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 at 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 residents of Oregon: State law advises you to report any suspected identity theft to law enforcement, including the Attorney General, and the Federal Trade Commission.

For residents of Rhode Island: It is required by state law that you are informed of your right to file or obtain a police report in regard to this incident.

For residents of Arizona, Colorado, District of Columbia, Illinois, Maryland, New York, North Carolina, and Rhode Island: You can obtain information from the Offices of the Attorney General and the Federal Trade Commission about fraud alerts, security freezes, and steps you can take toward preventing identity theft.

Federal Trade Commission - Consumer Response Center: 600 Pennsylvania Ave, NW, Washington, DC 20580; 1-877-IDTHEFT (438-4338); www.identitytheft.gov

Arizona Office of the Attorney General Consumer Protection & Advocacy Section, 2005 North Central Avenue, Phoenix, AZ 85004 1-602-542-5025

Colorado Office of the Attorney General Consumer Protection 1300 Broadway, 9th Floor, Denver, CO 80203 1-720-508-6000 www.coag.gov

District of Columbia Office of the Attorney General – Office of Consumer Protection: 400 6th Street, NW, Washington, DC 20001; 202-727-3400; www.oag.dc.gov

Illinois office of the Attorney General - 100 West Randolph Street, Chicago, IL 60601; 1-866-999-5630; www.illinoisattorneygeneral.gov

Maryland Office of the Attorney General - Consumer Protection Division: 200 St. Paul Place, 16th floor, Baltimore, MD 21202; 1-888-743-0023; www.oag.state.md.us

New York Office of Attorney General - Consumer Frauds & Protection: The Capitol, Albany, NY 12224; 1-800-771-7755; <https://ag.ny.gov/consumer-frauds/identity-theft>

North Carolina Office of the Attorney General - Consumer Protection Division: 9001 Mail Service Center, Raleigh, NC 27699; 1-877-566-7226; www.ncdoj.com

Rhode Island Office of the Attorney General - Consumer Protection: 150 South Main St., Providence RI 02903; 1-401-274-4400; www.riag.ri.gov.