

CIPRIANI & WERNER

A PROFESSIONAL CORPORATION

ATTORNEYS AT LAW

CAITLIN LAWLOR
CLawlor@c-wlaw.com

450 Sentry Parkway, Suite 200
Blue Bell, PA 19422

Phone: (610) 567-0700
Fax: (610) 567-0712

www.C-WLAW.com

A Mid-Atlantic Litigation Firm

Visit us online at
www.C-WLAW.com

November 8, 2024

Via E-Mail (IDTheft@oag.state.md.us)

Office of the Attorney General
200 St. Paul Place
Baltimore, Maryland 21202

RE: Data Incident Notification

To Whom It May Concern:

We serve as counsel for Fairfield University located at 1073 North Benson Road, Fairfield, CT 06824. We write to provide notification of a recent data security incident. By providing this notice, Fairfield does not waive any rights or defenses under Maryland law, including the data breach notification statute.

On February 29, 2024, Fairfield University ("Fairfield") discovered suspicious activity related to certain faculty email accounts. Upon discovery, Fairfield took swift action to secure its email system and network, and immediately began an internal investigation. Fairfield also engaged third-party forensic specialists to investigate the full nature and scope of the incident. Based on the investigation, it was determined that certain Fairfield faculty email accounts were subject to unauthorized access. As a result, together with third-party specialists, Fairfield began a comprehensive review of the contents of these accounts to determine the type of information contained therein and to whom that information related. This comprehensive review was completed on October 3, 2024.

At that time, Fairfield determined that information related to 4 Maryland residents may have been subject to unauthorized access. The information believed to be at risk may include a first and last name, in combination with a Social Security number, passport number, and/or medical diagnosis or treatment information.

On November 4, 2024, Fairfield sent written notice of this incident to the potentially impacted Maryland residents pursuant to Maryland law. The notice letter included an offer of complimentary credit monitoring and identity protection services for 12 months. The notice letter sent to individuals is substantially similar to the letter attached hereto as "**Exhibit A.**"

Please contact me should you have any questions.

Very truly yours,



Caitlin Lawlor, Esq.
CIPRIANI & WERNER, P.C.

EXHIBIT A



November 4, 2024

NOTICE OF DATA BREACH

Dear [REDACTED]:

We are writing to inform you of a cyber security incident experienced by Fairfield University ("Fairfield") that may have involved your information described below. While we have no evidence of attempted or actual misuse of any information, we are providing you with information about the incident, our response, and steps you can take to help protect your information, should you feel it appropriate to do so.

What Happened: On February 29, 2024, we discovered suspicious activity related to certain faculty email accounts. Upon discovery, we took swift action to secure our email system and network, and immediately began an internal investigation. We also engaged third-party forensic specialists to investigate the full nature and scope of the incident. Based on the investigation, it was determined that certain Fairfield faculty email accounts were subject to unauthorized access. As a result, together with third-party specialists, we began a comprehensive review of the contents of these accounts to determine the type of information contained therein and to whom that information related. This comprehensive review was completed on October 3, 2024. We are now notifying those individuals whose information was potentially impacted by the incident.

What Information Was Involved: The information believed to potentially be at risk includes your first and last name, in combination with your [REDACTED]

What We Are Doing: Upon discovery, we immediately began an internal investigation and engaged third-party forensic specialists to investigate this matter. Out of an abundance of caution, we have arranged for you to activate, at no cost to you, Single Bureau Credit Monitoring/Single Bureau Credit Report/Single Bureau Credit Score services. These services provide you with alerts for twelve (12) months from the date of enrollment when changes occur to your credit file. This notification is sent to you the same day that the change or update takes place with the bureau. Finally, we are providing you with proactive fraud assistance to help with any questions that you might have. These services will be provided by Cyberscout, a TransUnion company, specializing in fraud assistance and remediation services. Due to privacy laws, we cannot activate these services for you directly. Additional information regarding how to activate the complimentary identity monitoring service is enclosed. We have also provided additional information about steps you can take to help protect yourself against fraud and identity theft.

What You Can Do: We recommend that you remain vigilant in regularly reviewing and monitoring all of your account statements and credit history to guard against any unauthorized transactions or activity. If you discover any suspicious or unusual activity on your accounts, please promptly contact your financial institution or company. Additionally, you can enroll to receive the complimentary identity monitoring services we are making available to you. You can also review the enclosed "Steps You Can Take to Help Protect Your Information" for additional resources.

For More Information: Should you have additional questions or concerns regarding this matter, please do not hesitate to contact our dedicated call center agents at 1-800-405-6108 during the hours of 8:00 a.m. to 8:00 p.m. Eastern time, Monday through Friday, excluding holidays. You may also write to us at 1073 North Benson Road, Fairfield, CT 06824.

We take the privacy and security of the information in our care seriously, and sincerely regret any worry or inconvenience this incident may cause you and your family.

Sincerely,

A handwritten signature in cursive script, appearing to read "JoAnne Williams".

JoAnne Williams
Senior Vice President

STEPS YOU CAN TAKE TO HELP PROTECT YOUR INFORMATION

How do I enroll for the free services?

To enroll in Credit 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:



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.



ADDITIONAL ACTIONS TO HELP PROTECT YOUR INFORMATION

Monitor Your Accounts

We encourage you to remain vigilant against incidents of identity theft and fraud by reviewing your credit reports/account statements for suspicious activity and to detect errors. Under U.S. law, you are entitled to one free credit report annually from each of the three major credit reporting bureaus, TransUnion, Experian, and Equifax. To order your free credit report, visit www.annualcreditreport.com or call 1-877-322-8228. Once you receive your credit report, review it for discrepancies and identify any accounts you did not open or inquiries from creditors that you did not authorize. If you have questions or notice incorrect information, contact the credit reporting bureau.

You have the right to place an initial or extended “fraud alert” on a credit file at no cost. An initial fraud alert is a one-year alert that is placed on a consumer’s credit file. Upon seeing a fraud alert, 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 lasting seven years. Should you wish to place a fraud alert, please contact any of the three credit reporting bureaus listed below.

As an alternative to a fraud alert, you have the right to place a “credit freeze” on a credit report, which will prohibit a credit bureau from releasing information in the credit report without your express authorization. The credit 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 credit freeze 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 credit freeze on your credit report. To request a credit freeze, you will need to provide the following information:

1. Full name (including middle initial as well as Jr., Sr., III, etc.);
2. Social Security number;
3. Date of birth;
4. Address for the prior two to five years;
5. Proof of current address, such as a current utility or telephone bill;
6. A legible photocopy of a government-issued identification card (e.g., state driver’s license or identification card); and
7. A copy of either the police report, investigative report, or complaint to a law enforcement agency concerning identity theft, if you are a victim of identity theft.

Should you wish to place a fraud alert or credit freeze, please contact the three major credit reporting bureaus listed below:

TransUnion 1-800-680-7289 www.transunion.com TransUnion Fraud Alert P.O. Box 2000 Chester, PA 19016-2000 TransUnion Credit Freeze P.O. Box 160 Woodlyn, PA 19094	Experian 1-888-397-3742 www.experian.com Experian Fraud Alert P.O. Box 9554 Allen, TX 75013 Experian Credit Freeze P.O. Box 9554 Allen, TX 75013	Equifax 1-888-298-0045 www.equifax.com Equifax Fraud Alert P.O. Box 105069 Atlanta, GA 30348-5069 Equifax Credit Freeze P.O. Box 105788 Atlanta, GA 30348-5788
---	---	--

Additional Information

You can further educate yourself regarding identity theft, fraud alerts, credit freezes, and the steps you can take to protect your personal information by contacting the credit reporting bureaus, the Federal Trade Commission (FTC), or your state Attorney General. The FTC also encourages those who discover that their information has been misused to file a complaint with them. The FTC may be reached at 600 Pennsylvania Ave. NW, Washington, D.C. 20580; www.identitytheft.gov; 1-877-ID-THEFT (1-877-438-4338); and TTY: 1-866-653-4261.

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, your state Attorney General, and the FTC. This notice has not been delayed by law enforcement.

For Maryland residents, the Maryland Attorney General may be contacted at: 200 St. Paul Place, 16th Floor, Baltimore, MD 21202; 1-410-528-8662 or 1-888-743-0023; and <https://www.marylandattorneygeneral.gov/>. Fairfield University may be contacted at 1073 North Benson Road, Fairfield, CT 06824.

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

For Rhode Island residents, the Rhode Island Attorney General may be reached at: 150 South Main Street, Providence, RI 02903; 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 are 2 Rhode Island residents impacted by this incident.