April 4, 2024

Via Certified Mail; Return Receipt Requested

Attorney General John Formella
Office of the New Hampshire Attorney General
Attn: Security Breach Notification
33 Capitol Street
Concord, NH 03301

Notice Re: Data Security Incident Involving The Bernstein Companies

Dear Attorney General Formella:

Wilson Elser Moskowitz Edelman and Dicker LLP ("Wilson Elser") represents The Bernstein Companies ("TBC"), a diversified real estate investment, consulting, and management company located at 3299 K Street NW, Suite 700, Washington, D.C. 20007, with respect to a recent cybersecurity incident that was first discovered by TBC on December 29, 2023 (hereinafter, the "Incident"). TBC takes the security and privacy of the information in its control very seriously and has taken steps to prevent a similar incident from occurring in the future.

1. Nature of the Incident

On December 29, 2023, TBC discovered unauthorized activity within its network that may have resulted in unauthorized access to sensitive information of employees of TBC, employees of Bernstein Management Associates, and its business venture investors. Upon discovery of the Incident, TBC promptly engaged a specialized cybersecurity incident response vendor to secure its network and conduct a forensic investigation to determine the source and scope of the unauthorized activity. On or about January 23, 2024, the forensic investigation confirmed unauthorized activity within TBC's network.

Based on these findings, TBC began reviewing the affected systems to identify the specific individuals and the types of information that may have been compromised. While the review was ongoing, on February 12, 2024, TBC posted a notice of the Incident on the homepage of its website and, on February 14, 2024, published a notice of the Incident with The Baltimore Sun Daily, a newspaper printed and published in Baltimore City and/or Baltimore County.

TBC completed its review of the impacted data on February 21, 2024. Upon completion of its review, TBC engaged a thirty-party mailing vendor to assist with mailing notice letters to the affected individuals, providing a ninety (90) day call center for individuals to contact should they

have additional questions regarding the Incident, and provide complimentary credit monitoring and identity theft protection services to the affected individuals.

2. What Information Was Involved?

TBC has determined that the following types of personally identifiable information may have been impacted: [redacted] may have also been impacted in the Incident. The information impacted varies by individual.

Please note that to date there has been no evidence to indicate that any individuals' personal information has been misused as a result of the Incident.

3. Number of New Hampshire residents affected.

Upon completion of its review, TBC determined that information pertaining to two (2) New Hampshire residents were impacted as a result of the Incident. Notification letters to these individuals were mailed on April 2, 2024, by first class mail. A sample copy of the notification letter is attached hereto as **Exhibit A**.

4. Steps taken in response to the Incident.

TBC is committed to ensuring the security and privacy of all personal information within its control and is taking steps to prevent a similar incident from occurring in the future. Upon discovery of the Incident, TBC moved quickly to investigate and respond to the Incident and assessed the security of its systems. Specifically, TBC engaged a specialized cybersecurity firm to conduct a forensic investigation to determine the nature and scope of the Incident. Additionally, TBC continues to enhance its network security to prevent a similar incident from occurring in the future, including adding additional restrictions to access accounts, implementing two factor authentication on all corporate accounts, and disabling remote desktop and remote PowerShell on all domain computers. TBC also implemented additional security software, monitoring services, and protocols to prevent and identify vulnerabilities to prevent future incidents. Lastly, TBC informed our law firm and began identifying the potentially affected individuals in preparation for notice.

Although TBC is not aware of any actual or attempted misuse of the affected personal information, TBC offered [redacted] of complimentary credit monitoring and identity theft restoration services through Identity Force, a TransUnion company, to the impacted individuals residing in State of New Hampshire to help protect their identity. Additionally, TBC provided guidance on how to better protect against identity theft and fraud, provide 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.

5. Contact information

TBC 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 J[redacted]

Very truly yours,

Wilson Elser Moskowitz Edelman & Dicker LLP

[redacted]

Jennifer S. Stegmaier

EXHIBIT A

The Bernstein Companies
c/o Cyberscout
PO Box 1286
Dearborn, MI 48120-9998

THE BERNSTEIN COMPANIES

P
[redacted]

March 12, 2024

VIA FIRST-CLASS MAIL

0000101102G0400

P

Notice of Data Breach

Dear [redacted],

The Bernstein Companies ("TBC") is writing to inform you of a recent data security impacting its systems that may have resulted in unauthorized access to sensitive information of employees of TBC, employees of Bernstein Management Associates ("BMA"), and its business venture investors. TBC takes the privacy of client information very seriously and sincerely apologizes for any inconvenience this Incident may cause. This letter contains details about the Incident, steps we have taken in response to mitigate any risk, and services we are making available to protect your information.

What Happened?

On December 29, 2023, TBC discovered unauthorized activity within its network. Upon discovery of the Incident, TBC promptly engaged a specialized cybersecurity incident response firm to secure its network and conduct a forensic investigation to determine the source and scope of the unauthorized activity. On January 23, 2024, the forensic investigation confirmed unauthorized activity within TBC's network. Based on these findings, TBC began reviewing the affected systems to identify the specific individuals and the types of information that may have been compromised for purposes of providing this notice.

What Information Was Involved?

Upon completion of its review, TBC confirmed that TBC and BMA employee personal information as well as investor personal information maintained within its computer systems may have been subject to unauthorized access. The data contained in this system may include your personal information such as your: [redacted]

Please note, at this time, there is no evidence to indicate that sensitive personal information has been misused as a result of this incident.

What We Are Doing

Data privacy and security is among TBC'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, TBC moved quickly to investigate, respond, and confirm the security of our systems. Specifically, TBC disconnected all access to our network, changed administrative credentials, restored operations in a safe and secure mode, enhanced the security measures, and took steps and will continue to take steps to mitigate the risk of future harm.

In light of the incident, we are also providing you with access to Single Bureau Credit Monitoring/Single Bureau Credit Report/Single Bureau Credit Score services at no charge. 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 or in the event that you become a victim of fraud.

These services will be provided by Cyberscout through Identity Force, a TransUnion company specializing in fraud assistance and remediation services. While we are covering the cost of these services, you will need to complete the activation process by following the instructions below.

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.

You may also activate the credit monitoring services we are making available to you at no cost. The deadline to enroll is June 13, 2024.

To enroll in Credit Monitoring services at no charge, please log on to [redacted] and follow the instructions provided. When prompted please provide the following unique code to receive services: [redacted]

The enrollment requires an internet connection and e-mail account and may not be available to minors under eighteen (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 information was misused. However, we encourage you to take full advantage of the services offered.

For More Information

If you have any questions or concerns not addressed in this letter, please call [redacted] (toll free) Monday through Friday, during the hours of 8:00 a.m. and 8:00 p.m. Eastern Time (excluding U.S. national holidays).

TBC sincerely regrets any concern or inconvenience this matter may cause, and remains dedicated to ensuring the privacy and security of all information in our control.

Sincerely,

Adam Bernstein
President & CEO
The Bernstein Companies

Steps You Can Take to Help Protect the Deceased's 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	**TransUnion**	**Equifax**
P.O. Box 9554	P.O. Box 2000	P.O. Box 105069
Allen, TX 75013	Chester, PA 19016	Atlanta, GA 30348
1-888-397-3742	1-800-680-7289	1-800-525-6285
www.experian.com/fraud/center.html	www.transunion.com/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.

Identity Protection PIN: You can get a six-digit Identity Protection PIN to prevent someone else from filing a tax return using your Social Security number or Individual Taxpayer Identification Number. An IP PIN is used by the IRS to verify your identity when filing your electronic or paper tax return. To receive an IP Pin, you must register to validate your identity at IRS.gov. Use the Get an IP PIN tool available between mid-January through mid-November to receive your IP PIN.

https://www.irs.gov/identity-theft-fraud-scams/get-an-identity-protection-pin

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	**TransUnion**	**Equifax**
P.O. Box 9554	P.O. Box 160	P.O. Box 105788
Allen, TX 75013	Woodlyn, PA 19094	Atlanta, GA 30348-5788
1-888-397-3742	1-888-909-8872	1-888-298-0045
www.experian.com/freeze/center.html	www.transunion.com/credit-freeze	https://www.equifax.com/personal/credit

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