



150 N. Riverside Plaza, Suite 3000, Chicago, IL 60606 • (312) 819-1900

February 18, 2022

Bruce A. Radke
312.463.6211
312.873.3763 Fax
bradke@polsinelli.com

Via Electronic Mail – Idtheft@oag.state.md.us

Office of the Attorney General
Attn: Jeff Karberg, Administrator of the Identity Theft Program
Attn: Security Breach Notification
200 St. Paul Place
Baltimore, MD 21202

Re: Notice of Data Breach

Dear Mr. Karberg,

We are writing to your office on behalf of our Client, Dunham & Associates Holdings, Inc. and its affiliates (hereafter, “Dunham” or “Client”). Dunham includes Dunham & Associates Investment Counsel, Inc., Dunham Trust Company, and Asset Managers, Inc. On or about October 29, 2021, Dunham learned that an unauthorized individual was able to access a Dunham email account (hereafter, the “Incident”). While within the account, the unauthorized individual sent spam email to a number of Dunham clients and business partners. While we are not aware of any instances of fraud or material risk to individual information, we are notifying your Office in an abundance of caution.

Polsinelli retained a specialized cybersecurity firm on behalf of Dunham to conduct a privileged investigation of the Incident. While the cybersecurity firm could not isolate the specific window of compromise of the relevant email account, based on the evidence available, the longest window of compromise possible would have been approximately August 2021 to November 20, 2021. Furthermore, there was no evidence to suggest that the unauthorized individual compromised any other of Dunham’s other email accounts or systems.

Typically, all sensitive financial information is submitted to Dunham through a secure portal. However, in an abundance of caution, Dunham retained an eDiscovery vendor to analyze the mailbox and determine whether any sensitive financial information was impacted. On or about December 21, 2021, the eDiscovery vendor confirmed that the account contained some sensitive personal information for approximately 198 individuals, 7 of which are residents of Maryland.

polsinelli.com

Atlanta Boston Chicago Dallas Denver Houston Kansas City Los Angeles Miami Nashville New York
Phoenix St. Louis San Francisco Seattle Silicon Valley Washington, D.C. Wilmington

Polsinelli PC, Polsinelli LLP in California



February 18, 2022

Page 2

Dunham has not discovered any specific evidence of fraud or identity theft. However, in an abundance of caution, Dunham will be providing credit monitoring services to potentially impacted individuals. A copy of the notice sent to the involved individuals is enclosed.

If you have any questions or concerns about the Incident, please do not hesitate to contact us.

Sincerely,

Bruce A. Radke

Enclosure



Return Mail Processing Center
P.O. Box 6336
Portland, OR 97228-6336

<<Mail ID>>
<<Name 1>>
<<Name 2>>
<<Address 1>>
<<Address 2>>
<<Address 3>>
<<Address 4>>
<<Address 5>>
<<City>> <<State>> <<Zip>>
<<Country>>

<<Date>>

Notice of Data Breach

Dear <<Name 1>>,

At Dunham & Associates Investment Counsel, Inc. and its affiliates, Dunham Trust Company and Asset Managers Inc. (collectively “Dunham”), we strive to provide exceptional client service for the financial advisors, clients and trusted partners we work with. The foundation of our partnership is based on trust, and that requires honest, transparent, and direct communication. We are reaching out to inform you that we recently experienced a data security incident that may have involved some of your personal information.

What Happened. Dunham is committed to the privacy of individuals and takes the protection of personal information that is entrusted to us seriously. Although we have no evidence or reason to believe that your information has been used to commit fraud or identity theft, we recently discovered on November 17, 2021, that beginning on or about October 22, 2021, or earlier, someone outside of Dunham temporarily accessed an employee email account without authorization. While the cybersecurity firm engaged could not isolate the specific window of compromise of the relevant email account, based on the evidence available, the longest window of compromise possible would have been approximately August 2021 to November 20, 2021.

Based on our investigation, there is no evidence to suggest that the compromise extended beyond the email system. There was no evidence of access to the Client Portal, where account information is displayed to financial advisors and clients.

What We Are Doing. Upon learning of the situation, the firm promptly contained the incident by securing the account to prevent further access, the email account was immediately disabled, and all affected user passwords reset. We immediately began an initial internal investigation into the incident and promptly, in conjunction with counsel, engaged a leading cybersecurity firm to conduct a comprehensive forensic investigation of the incident to confirm the security of our computer systems and network.

On December 21, 2021, our investigation determined that the email account contained some of your personal information. We have no reason to believe that client data was the intended target of the incident and have no indication that any such information has been used for fraud or identity theft purposes. Nonetheless we are providing you with this notice because your personal information may have been contained in the relevant account. We are also committed to taking steps to help prevent something like this from happening again, including reviewing our technical and security controls.

Although we are not aware of any instances of fraud or identity theft, we are offering a complimentary <<one/two>>-year membership of Experian IdentityWorksSM Credit 3B. This product helps detect possible misuse of your personal information and provides you with identity protection services focused on immediate identification and resolution of identity theft. IdentityWorks Credit 3B is completely free to you, and enrolling in this program will not hurt your credit score. **For more information on identity theft prevention and IdentityWorks Credit 3B, including instructions on how to activate your complimentary <<one/two>>-year membership, please see the additional information provided in this letter.**

What Information Was Involved. As part of our investigation, we searched for any personal information that could have been viewed. Based on our investigation, the following data elements were present in the mailbox: <<Data Elements>>. To confirm, we are not aware of any instances of fraud as a result of the Incident.

What You Can Do. As a precautionary measure, we recommend that you remain vigilant to protect against potential fraud and/or identity theft by, among other things, reviewing your account statements and monitoring credit reports closely. If you detect any suspicious activity on an account, you should promptly notify the financial institution or company with which the account is maintained. You should also promptly report any fraudulent activity or any suspected incidents of identity theft to proper law enforcement authorities, including the police and your state's attorney general, as well as the Federal Trade Commission ("FTC").

For More Information. Please call Dunham at (800) 442-4358 or (858) 964-0500 from 8:00 a.m. to 5:00 p.m. PT.

We sincerely apologize for any inconvenience or concern this incident might cause. We take our responsibility to safeguard your personal information seriously and have taken the necessary steps to strengthen our security protocols. Thank you for your continued trust you have placed in our firm.

Sincerely,



Jeffrey A. Dunham
President
Dunham & Associates

Additional Important Information

FTC Contact Information. You may wish to review the tips provided by the FTC on fraud alerts, security/credit freezes and steps to you can take to avoid identity theft. For more information and to contact the FTC, please visit www.ftc.gov/idtheft or call 1-877-ID-THEFT (1-877-438-4338). You may also contact the FTC at: Federal Trade Commission, 600 Pennsylvania Avenue, NW, Washington, DC 20580.

Credit Reports. You may obtain a free copy of your credit report once every 12 months from each of the three national credit reporting agencies by visiting <http://www.annualcreditreport.com>, by calling toll-free 1-877-322-8228, or by completing an Annual Credit Report Request Form and mailing it to Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA 30348. You can print a copy of the request form at <https://www.annualcreditreport.com/cra/requestformfinal.pdf>.

Alternatively, you may elect to purchase a copy of your credit report by contacting one of the three national credit reporting agencies listed below. Contact information for the three national credit reporting agencies for the purpose of requesting a copy of your credit report or for general inquiries, including obtaining information about fraud alerts and placing a security freeze on your credit files, is as follows:

Equifax 1-800-349-9960 www.equifax.com P.O. Box 105788 Atlanta, GA 30348	Experian 1-888-397-3742 www.experian.com P.O. Box 9554 Allen, TX 75013	TransUnion 1-888-909-8872 www.transunion.com P.O. Box 2000 Chester, PA 19022
---	--	--

Fraud Alerts. You may want to consider placing a fraud alert on your credit report. An initial fraud alert is free and will stay on your credit file for at least 90 days. The alert informs creditors of possible fraudulent activity within your report and requests that the creditor contact you prior to establishing any new accounts in your name. To place a fraud alert on your credit report, contact any of the three national credit reporting agencies using the contact information listed above. Additional information is available at <http://www.annualcreditreport.com>.

Credit and Security Freezes. You may have the right to place a credit freeze, also known as a security freeze, on your credit file, so that no new credit can be opened in your name without the use of a PIN number that is issued to you when you initiate the freeze. A credit freeze is designed to prevent potential credit grantors from accessing your credit report without your consent. If you place a credit freeze, potential creditors and other third parties will not be able to get access to your credit report unless you temporarily lift the freeze. Therefore, using a credit freeze may delay your ability to obtain credit. Unlike a fraud alert, you must separately place a credit freeze on your credit file at each credit reporting company. Since the instructions for how to establish a credit freeze differ from state to state, please contact the three major credit reporting companies as specified below to find out more information:

Equifax Security Freeze 1-800-349-9960 www.equifax.com P.O. Box 105788 Atlanta, GA 30348	Experian Security Freeze 1-888-397-3742 www.experian.com P.O. Box 9554 Allen, TX 75013	TransUnion Security Freeze 1-888-909-8872 www.transunion.com P.O. Box 160 Woodlyn, PA 19094
---	--	---

In order to request a security freeze, you may need to provide the following information:

1. Your full name (including middle initial as well as Jr., Sr., II, III, etc.);
2. Social Security Number;
3. Date of birth;
4. If you have moved in the past five (5) years, provide the addresses where you have lived over the prior five years;
5. Proof of current address such as a current utility bill or telephone bill;
6. A legible photocopy of a government issued identification card (state driver's license or ID card, military identification, etc.);
7. 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.

The credit reporting agencies have three (3) business days after receiving your request to place a security freeze on your credit report. The credit bureaus must also send written confirmation to you within five (5) business days and provide you with a unique personal identification number (PIN) or password, or both that can be used by you to authorize the removal or lifting of the security freeze.

To remove the security freeze or lift the freeze in order 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** the PIN number or password provided to you 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 three (3) business days after receiving your request to remove or lift the security freeze for those identified entities or for the specified period of time.

If you do not have internet access but would like to learn more about how to place a security freeze on your credit report, California residents may contact the California Attorney General's Office at (916) 445-9555. Maryland residents may contact the Maryland Attorney General at 1-(888)-743-0023.

Individuals interacting with credit reporting agencies have rights under the Fair Credit Reporting Act. We encourage you to review your rights under the Fair Credit Reporting Act by visiting www.consumerfinance.gov/f/201504_cfpb_summary_your-rights-under-fcra.pdf, or by requesting information in writing from the Consumer Response Center, Room 130-A, Federal Trade Commission, 600 Pennsylvania Ave. NW, Washington, DC 20580.

This notice was not delayed due to a law enforcement delay.

ACTIVATING YOUR COMPLIMENTARY CREDIT MONITORING

To help protect your identity, we are offering a **complimentary** <<one/two>>-year membership of Experian IdentityWorksSM Credit 3B. This product helps detect possible misuse of your personal information and provides you with superior identity protection support focused on immediate identification and resolution of identity theft.

Activate IdentityWorks Credit 3B Now in Three Easy Steps

1. ENROLL by: <<Enrollment Deadline>> (Your code will not work after this date.)
2. VISIT the Experian IdentityWorks website to enroll: <https://www.experianidworks.com/3bcredit>
3. PROVIDE the Activation Code: <<Activation Code>>

If you have questions about the product, need assistance with identity restoration or would like an alternative to enrolling in Experian IdentityWorks online, please contact Experian's customer care team at 877-288-8057. Be prepared to provide engagement number <<Engagement Number>> as proof of eligibility for the identity restoration services by Experian.

ADDITIONAL DETAILS REGARDING YOUR <<12/24>>-MONTH EXPERIAN IDENTITYWORKS CREDIT 3B MEMBERSHIP:

A credit card is **not** required for enrollment in Experian IdentityWorks Credit 3B.

You can contact Experian **immediately** regarding any fraud issues, and have access to the following features once you enroll in Experian IdentityWorks:

- **Experian credit report at signup:** See what information is associated with your credit file. Daily credit reports are available for online members only.*
- **Credit Monitoring:** Actively monitors Experian, Equifax and Transunion files for indicators of fraud.
- **Identity Restoration:** Identity Restoration specialists are immediately available to help you address credit and non-credit related fraud.
- **Experian IdentityWorks ExtendCARETM:** You receive the same high-level of Identity Restoration support even after your Experian IdentityWorks membership has expired.
- **Up to \$1 Million Identity Theft Insurance^{**}:** Provides coverage for certain costs and unauthorized electronic fund transfers.

Activate your membership today at <https://www.experianidworks.com/3bcredit> or call 877-288-8057 to register with the activation code above.

What you can do to protect your information: There are additional actions you can consider taking to reduce the chances of identity theft or fraud on your account(s). Please refer to www.ExperianIDWorks.com/restoration for this information. 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 care team at 877-288-8057.

* Offline members will be eligible to call for additional reports quarterly after enrolling.

** 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.