



MULLEN
COUGHLIN LLC
ATTORNEYS AT LAW

Edward J. Finn
Office: (267) 930-4776
Fax: (267) 930-4771
Email: efinn@mullen.law

426 W. Lancaster Avenue, Suite 200
Devon, PA 19333

January 7, 2021

VIA U.S. MAIL

Consumer Protection Bureau
Office of the New Hampshire Attorney General
33 Capitol Street
Concord, NH 03301

Re: Notice of Data Event

Dear Sir or Madam:

We represent Thornburg Investment Management, Inc. (“Thornburg”) located at 2300 North Ridgeway Road Santa Fe, NM 87506, and are writing to notify your office of an incident that may affect the security of some personal information relating to fourteen (14) New Hampshire residents. Thornburg reserves the right to supplement this notice with any new significant facts learned subsequent to its submission. By providing this notice, Thornburg does not waive any rights or defenses regarding the applicability of New Hampshire law, the applicability of the New Hampshire data event notification statute, or personal jurisdiction.

Nature of the Data Event

On or about April 13, 2021, Thornburg became aware of suspicious activity related to certain Thornburg employee email accounts and promptly launched an investigation to determine the nature and scope of the incident and to remediate the issue. Thornburg later became aware of additional suspicious activity on April 30, 2021, and promptly conducted an additional investigation into the subsequent suspicious activity. The investigations determined that there was unauthorized access to certain employee email accounts for a varying period of time between March 29, 2021 and April 30, 2021. While the investigations did not reveal evidence that any specific emails or attachments within the accounts were viewed or taken by an unauthorized individual, the investigation was unable to rule that out. Accordingly, Thornburg completed a review of the at-risk contents of the email accounts with the assistance of third-party data mining specialists to determine whether any sensitive information could have been obtained by the threat actor(s). On September 30, 2021, Thornburg completed the review of the impacted email accounts. Thereafter, Thornburg provided notice of the incident to various data owners and/or intermediaries and obtained addresses needed to provide notice to those potentially impacted. Thornburg recently completed its coordination with those various parties.

The information that could have been subject to unauthorized access varies by individual and includes name, Social Security number, and financial account information.

Notice to New Hampshire Residents

On or about January 7, 2022, Thornburg began providing written notice of this incident to affected individuals, which includes approximately fourteen (14) New Hampshire residents. Thornburg continues to work with data owners/intermediaries and an additional wave of notice will be sent to a small number of individuals. Written notice is being provided in substantially the same form as the letter attached here as *Exhibit A*.

Other Steps Taken and To Be Taken

Upon discovering the event, Thornburg moved quickly to investigate and respond to the incident, assess the security of Thornburg systems, and notify potentially affected individuals. Thornburg has put in place additional measures aimed to prevent a phishing attempt or compromise of its email systems in the future. Thornburg also notified law enforcement of the event. Thornburg is providing access to credit monitoring services for twelve (12) months through Equifax to individuals whose personal information was potentially affected by this incident, at no cost to these individuals.

Additionally, Thornburg is providing impacted individuals with guidance on how to better protect against identity theft and fraud, including advising individuals to monitor account statements and credit reports over the next 12 – 24 months and to report any suspected incidents of identity theft or fraud to their credit card company and/or bank. Thornburg is providing individuals with 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 encouragement to contact the Federal Trade Commission, their state Attorney General, and law enforcement to report attempted or actual identity theft and fraud.

Contact Information

Should you have any questions regarding this notification or other aspects of the data security event, please contact us at (267) 930-4776.

Very truly yours,



Edward J. Finn of
MULLEN COUGHLIN LLC

EJF/smm

EXHIBIT A



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 <<VARIABLE HEADER>>

Dear <<Name 1>>:

Thornburg Investment Management, Inc. (“Thornburg” or “we”) is writing on behalf of <<ENTITY>> to inform you of an incident that potentially impacted the security of your information. While Thornburg does not have evidence that your information has or will be misused, we are writing to provide you with information about this incident and steps you can take to better protect yourself against the possibility of identity theft and fraud, should you feel it is appropriate to do so.

What Happened? On or around April 13, 2021, Thornburg became aware of suspicious activity related to certain Thornburg employee email accounts and we promptly launched an investigation to determine the nature and scope of the incident and to remediate the issue. We later became aware of additional suspicious activity on April 30, 2021, and promptly conducted an additional investigation into the subsequent suspicious activity. The investigations determined that there was unauthorized access to certain employee email accounts for a varying period of time between March 29, 2021 and April 30, 2021. While the investigations did not reveal evidence that any specific emails or attachments within the accounts were viewed or taken by an unauthorized individual, we are unable to rule that out. Accordingly, we completed a review of the at-risk contents of the email accounts to determine whether any sensitive information could have been obtained by the threat actor(s). On September 30, 2021, Thornburg completed the review of the impacted email accounts. Thereafter, Thornburg obtained addresses needed to provide notice to those potentially impacted.

What Information Was Involved? The investigation determined that your name and the following types of your information may have been impacted by this incident: <<Data Elements>>. At this time, we have not received reports of actual or attempted misuse of any personal information as a result of this incident.

What We Are Doing. The privacy and security of information in our possession is one of our highest priorities. Upon discovery, Thornburg promptly launched an internal investigation to determine the scope of the incident. Thornburg has put in place additional measures aimed to prevent a phishing attempt or compromise of our email systems in the future. Thornburg also notified law enforcement of the incident. As an added precaution, we are offering you access to complimentary credit monitoring and identity restoration services through Equifax for a period of <<CM Length>> months. Individuals who wish to receive these services must enroll by following the attached enrollment instructions.

What You Can Do. We encourage you to remain vigilant against incidents of identity theft and fraud by reviewing your account statements and monitoring your free credit reports over the next 12 – 24 months for suspicious activity and to detect errors. You can also review the enclosed *Steps You Can Take to Protect Personal Information*, which contains information on what you can do to better protect against the possibility of identity theft and fraud should you feel it is appropriate to do so. There you will also find more information on the credit monitoring and identity restoration services we are offering and the steps you can take to enroll to receive them.

For More Information. We sincerely regret any inconvenience or concern this may have caused you. We understand you may have questions that are not answered in this letter. To ensure your questions are answered in a timely manner, you can call us at 800-847-0200, Monday through Friday, 7:30 a.m. to 3:30 p.m. Mountain Time, or write to Thornburg at 2300 North Ridgetop Road, Santa Fe, NM 87506.

Sincerely,

Thornburg Investment Management, Inc.

STEPS YOU CAN TAKE TO PROTECT PERSONAL INFORMATION

Enroll in Complimentary Credit Monitoring

As a safeguard, we have arranged for you to enroll, at no cost to you, in an online credit monitoring service for <<CM Length>> months provided by Equifax. The deadline to enroll in these services is <<Enrollment Date>>.

Key Features of the Monitoring Product

- Credit monitoring with email notifications of key changes to your Equifax credit report
- Daily access to your Equifax credit report
- WebScan notifications¹ when your personal information, such as Social Security Number, credit/debit card or bank account numbers are found on fraudulent Internet trading sites
- Automatic fraud alerts², which encourages potential lenders to take extra steps to verify your identity before extending credit, plus blocked inquiry alerts and Equifax credit report lock³
- Identity Restoration to help restore your identity should you become a victim of identity theft, and a dedicated Identity Restoration Specialist to work on your behalf
- Up to \$1,000,000 of identity theft insurance coverage for certain out of pocket expenses resulting from identity theft⁴

Enrollment Instructions

Go to www.equifax.com/activate

Enter your unique Activation Code of <<ACTIVATION CODE>> then click "Submit" and follow these 4 steps:

1. **Register:**
Complete the form with your contact information and click "Continue".
If you already have a myEquifax account, click the 'Sign in here' link under the "Let's get started" header. Once you have successfully signed in, you will skip to the Checkout Page in Step 4.
 2. **Create Account:**
Enter your email address, create a password, and accept the terms of use.
 3. **Verify Identity:**
To enroll in your product, we will ask you to complete our identity verification process.
 4. **Checkout:**
Upon successful verification of your identity, you will see the Checkout Page.
Click 'Sign Me Up' to finish enrolling.
- You're done!**
The confirmation page shows your completed enrollment.
Click "View My Product" to access the product features.

¹WebScan searches for your Social Security Number, up to 5 passport numbers, up to 6 bank account numbers, up to 6 credit/debit card numbers, up to 6 email addresses, and up to 10 medical ID numbers. WebScan searches thousands of Internet sites where consumers' personal information is suspected of being bought and sold, and regularly adds new sites to the list of those it searches. However, the Internet addresses of these suspected Internet trading sites are not published and frequently change, so there is no guarantee that we are able to locate and search every possible Internet site where consumers' personal information is at risk of being traded.

²The Automatic Fraud Alert feature is made available to consumers by Equifax Information Services LLC and fulfilled on its behalf by Equifax Consumer Services LLC.

³Locking your Equifax credit report will prevent access to it by certain third parties. Locking your Equifax credit report will not prevent access to your credit report at any other credit reporting agency. Entities that may still have access to your Equifax credit report include: companies like Equifax Global Consumer Solutions, which provide you with access to your credit report or credit score, or monitor your credit report as part of a subscription or similar service; companies that provide you with a copy of your credit report or credit score, upon your request; federal, state and local government agencies and courts in certain circumstances; companies using the information in connection with the underwriting of insurance, or for employment, tenant or background screening purposes; companies that have a current account or relationship with you, and collection agencies acting on behalf of those whom you owe; companies that authenticate a consumer's identity for purposes other than granting credit, or for investigating or preventing actual or potential fraud; and companies that wish to make pre-approved offers of credit or insurance to you. To opt out of such pre-approved offers, visit www.optoutprescreen.com.

⁴The Identity Theft Insurance benefit is underwritten and administered by American Bankers Insurance Company of Florida, an Assurant company, under group or blanket policies issued to Equifax, Inc., or its respective affiliates for the benefit of its Members. Please refer to the actual policies for terms, conditions, and exclusions of coverage. Coverage may not be available in all jurisdictions.

Monitor Your Accounts

Under U.S. law, a consumer is entitled to one free credit report annually from each of the three major credit reporting bureaus, Equifax, Experian, and TransUnion. To order your free credit report, visit www.annualcreditreport.com or call, toll-free, 1-877-322-8228. You may also directly contact the three major credit reporting bureaus listed below to request a free copy of your credit report.

Consumers have the right to place an initial or extended "fraud alert" on a credit file at no cost. An initial fraud alert is a 1-year alert that is placed on a consumer's credit file. Upon seeing a fraud alert display on a consumer's credit file, 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, which is a fraud alert lasting seven years. Should you wish to place a fraud alert, please contact any one of the three major credit reporting bureaus listed below. You can contact the credit reporting agencies to have fraudulent charges deleted.

As an alternative to a fraud alert, consumers 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 the consumer's 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 to take control over who gets access to the personal and financial information in your credit report 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 security freeze, you will need to provide the following information:

1. Full name (including middle initial as well as Jr., Sr., II, III, etc.);
2. Social Security number;
3. Date of birth;
4. Addresses for the prior two to 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, etc.); 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 credit freeze, please contact the three major credit reporting bureaus listed below:

Equifax	Experian	TransUnion
https://www.equifax.com/personal/credit-report-services/	https://www.experian.com/help/	https://www.transunion.com/credit-help
1-888-298-0045	1-888-397-3742	1-833-395-6938
Equifax Fraud Alert, P.O. Box 105069 Atlanta, GA 30348-5069	Experian Fraud Alert, P.O. Box 9554, Allen, TX 75013	TransUnion Fraud Alert, P.O. Box 2000, Chester, PA 19016
Equifax Credit Freeze, P.O. Box 105788 Atlanta, GA 30348-5788	Experian Credit Freeze, P.O. Box 9554, Allen, TX 75013	TransUnion Credit Freeze, P.O. Box 160, Woodlyn, PA 19094

Additional Information

You may further educate yourself regarding identity theft, fraud alerts, credit freezes, and the steps you can take to protect your personal information by contacting the consumer reporting bureaus, the Federal Trade Commission, or your state Attorney General. The Federal Trade Commission may be reached at: 600 Pennsylvania Avenue NW, Washington, DC 20580; www.identitytheft.gov; 1-877-ID-THEFT (1-877-438-4338); and 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. 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 and your state Attorney General. This notice has not been delayed by law enforcement.

For District of Columbia residents, the District of Columbia Attorney General may be contacted at: 400 6th St. NW, Washington, D.C. 20001; 202-727-3400; and oag@dc.gov.

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 www.oag.state.md.us. Thornburg is located at 2300 North Ridgetop Road, Santa Fe, NM 87506.

For New Mexico residents, 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 bureaus 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 by visiting 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 North Carolina residents, the North Carolina Attorney General may be contacted at: 9001 Mail Service Center, Raleigh, NC 27699-9001; 1-877-566-7226 or 1-919-716-6000; and www.ncdoj.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 36 Rhode Island residents impacted by this incident.

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/>.

MIH DEPT OF JUSTICE
JAN 12 2022 PM 12:57